4/2022

DVD Deutsche Vereinigung für Datenschutz e.V.

Datenschutz Nachrichten

45. Jahrgang
ISSN 0137-7767
14,00 Euro



■ Beschäftigtendatenschutzgesetz – was ist und was sein sollte ■ Beschäftigtendatenschutz aus gewerkschaftlicher Sicht ■ Datenschutz-Tätigkeitsberichte – eine Fundgrube auch für Beschäftigtenvertretungen ■ Ein Weg zur Umsetzung des neuen § 79a BetrVG ■ Personenbezogene Daten ohne Bedeutung? ■ Pressemitteilungen ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine



Samstag, 21.01.2023
DVD-Vorstandssitzung
online

Donnerstag, 26.01.2023
#PrivacyCamp23
EDRi mit VUB und IEE
https://privacycamp.eu/

Samstag, 28.01.2023
Europäischer Datenschutztag 2023

Mittwoch, 01.02.2023
Redaktionsschluss DANA 1/2023
„Europäische Entwicklungen"

Mittwoch/Donnerstag, 08./09.02.2023
16. Praxistage Datenschutz
vnr-Verlag, Köln

Freitag, 28.04.2023
BigBrotherAwards 2023
Bielefeld

Samstag, 29.04.2023
DVD-Vorstandssitzung
Bielefeld

Montag, 01.05.2023
Redaktionsschluss DANA 2/2023
„Europäische Entwicklungen"

Dienstag/Mittwoch, 09./10.05.2023
BvD-Verbandstage
Berlin

Montag – Mittwoch, 05.-07.06.2023
re:publica, Festival für die digitale Gesellschaft
Berlin (re-publica.com/de)

Montag/Dienstag, 12./13.06.2023
DuD-Datenschutzkongress 2023
Berlin

Foto: Pixabay..com

DANA
Datenschutz Nachrichten
ISSN 0137-7767
45. Jahrgang, Heft 4

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftsstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Thilo Weichert
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autorinnen und Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Dr.-Mack-Straße 83
90762 Fürth
www.onlineprinters.de
Tel. +49 (0) 9161 6209800
Fax +49 (0) 9161 8989 2000

Bezugspreis
Einzelheft 14 Euro. Jahresabonnement 48 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Nach einem Jahr kann das Abonnement jederzeit mit einer Frist von einem Monat gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta, Pixabay, iStock, Wikimedia Commons, Reinhard Linz.
Titel: iStock / Traitov

Editorial

Das ausgehende Jahr 2022 lieferte wenig Anlass zu Optimismus: Waren im Koalitionsvertrag der rot-grün-gelben Bundesregierung noch Signale zu erkennen, dass in Sachen Datenschutz nach langer schwarz-roter Agonie wenn nicht eine Zeiten-, so zumindest eine Trendwende stattfinden würde, so ist wieder Ernüchterung angesagt: Eine Innenministerin in Berlin betreibt das Ziel übermäßiger Vorratsdatenspeicherung; eine Innenkommissarin in Brüssel macht sich stark für eine europaweite Chat-Kontrolle. Ob dem genügend Widerstand in Politik, Gesellschaft und Justiz entgegengesetzt wird, bleibt offen.

Offen bleibt auch, ob das Versprechen des Koalitionsvertrags, endlich ein Beschäftigtendatenschutzgesetz in Kraft zu setzen, eingehalten werden wird. Dass dies immer dringlicher wird, zeigt dieses Heft, das sich dieses Themas aus den unterschiedlichsten Perspektiven annimmt: Dargestellt werden die Geschichte und praktisch zu regulierende Streitfragen (Schuler/Weichert), konkrete Forderungen von Gewerkschaftsseite (Wedde) sowie eher vage bleibende Ansätze eines Beirats zum Beschäftigtendatenschutz. Unsicherheit besteht in praktischen Fragen angesichts der Verantwortlichkeit des Arbeitgebers für die Datenverarbeitung des Betriebsrats (Schury/Piper). Die Aufsichtsbehörden sind gefordert (Köppen). Ein besonderer Fall der Arbeitnehmerdatenverarbeitung untermauert eine grundsätzliche Forderung, nämlich dass sich der Auskunftsanspruch der Betroffenen nicht allein auf die Art der über sie gespeicherten Daten beziehen darf, sondern auch die Algorithmen umfassen muss, die diese Daten verarbeiten (Linz). Datenübermittlungen in die USA bleiben ein Dauerproblem (Weichert). Auch nach Beendigung der beruflichen Tätigkeit hört die Datenverarbeitung nicht auf (Alenfelder).

Die vorliegende DANA wendet sich an die Politik und an die Praktiker:innen in Betriebsräten und Betrieben, denen mit den Beiträgen nicht nur Fragen, sondern auch Orientierungshilfen mitgegeben werden.

Der dicke Umfang des vorliegenden Heftes ist zwar nicht Ausdruck für die aktuelle Bedeutung des Datenschutzes in der aktuellen Politik – die auch mittelfristig vom Ukrainekrieg, der Klimakatastrophe und der Inflation bestimmt wird. Er ist aber wohl Ausdruck dafür, dass es in Sachen digitalen Grundrechtsschutzes an vielen Stellen in unserem Leben brennt. Die Meldungen aus Deutschland und der ganzen Welt sind hierfür Zeugnis.

Einigen dieser brennenden Konflikte hat sich die Europäische Union (EU) angenommen, was in den nächsten beiden DANAs im Jahr 2023 vertieft dargestellt werden wird. Sollte die Leser:in inspiriert sein, sich zu Aspekten der Digitalstrategien der EU in unserem Medium äußern zu wollen, so ist sie hiermit hierzu eingeladen das zu tun.

Die DANA-Redaktion

Autorinnen und Autoren dieser Ausgabe:

Heinz Alenfelder
DVD-Vorstandsmitglied, Köln,
alenfelder@datenschutzverein.de

Hajo Köppen
Rechtsanwalt, Gießen,
ra-koeppen@posteo.de

Dr. Reinhard Linz
DVD-Vorstandsmitglied, Bonn,
linz@datenschutzverein.de

Riko Piper
DVD-Vorstandsmitglied, Konzerndatenschutz Deutsche Flugsicherung, Langen,
pieper@datenschutzverein.de

Karin Schuler
Datenschutzberaterin für Betriebsräte, Netzwerk Datenschutzexpertise, Bonn,
karin@schuler-ds.de

Dr. Frank Schury
Konzern-Datenschutzbeauftragter der Deutschen Flugsicherung (DFS), Langen,
frank.schury@dfs.de

Prof. Dr. Peter Wedde
Beratungsgesellschaft d+a consulting GbR, Wiesbaden, peter.wedde@da-consulting.de

Dr. Thilo Weichert,
DVD-Vorstandsmitglied, Netzwerk Datenschutzexpertise, Kiel,
weichert@datenschutzverein.de

Karin Schuler/Thilo Weichert

Beschäftigtendatenschutzgesetz – was ist und was sein sollte

I. Ankündigungen

Die Hoffnung stirbt zuletzt; manchmal ist sie aber schon fast tot. Im rot-grün-gelben Koalitionsvertrag von 2021 steht:

Wir schaffen Regelungen zum Beschäftigtendatenschutz, um Rechtsklarheit für Arbeitgeber sowie Beschäftigte zu erreichen und die Persönlichkeitsrechte effektiv zu schützen.[1]

Wenig später nahm Arbeitsminister Hubertus Heil den Bericht des Beirats für ein Beschäftigtendatenschutzgesetz entgegen und erklärte:

Der Abschlussbericht des Beirats zum Beschäftigtendatenschutz kommt genau zum richtigen Zeitpunkt. Die neue Koalition will in dieser Legislatur Regelungen zum Beschäftigtendatenschutz schaffen, um Rechtsklarheit für Arbeitgeber und Beschäftigte zu erreichen und die Persönlichkeitsrechte der Beschäftigten effektiv zu schützen.[2]

Am 31.08.2022 legte aber Digitalminister Volker Wissing eine Digitalstrategie der Bundesregierung für die kommende Legislaturperiode vor. Hier hätte man eine Verortung des Vorhabens erwartet. Allerdings kann man sich des Eindrucks nicht erwehren, dass statt klarer Bekenntnisse das Prinzip „Rumeierei" verfolgt wird. In der Digitalstrategie heißt es unter anderem.

Wir werden mit modernen Regelungen zum Beschäftigtendatenschutz grundrechtswahrend und rechtssicher den Weg ebnen, um die Potenziale neuer Technologien für eine moderne Arbeitswelt zu nutzen.

Und weiter:

Wir wollen uns 2025 daran messen lassen, ob: (…) sich die Regeln für den Beschäftigtendatenschutz in der betrieblichen Praxis bewährt haben und aus Sicht aller Beteiligten zu mehr Rechtssicherheit beitragen.[3]

Abstrakter geht es kaum noch. Von einem klaren Bekenntnis zum Beschäftigtendatenschutzgesetz ist nichts zu erkennen.

Wer hoffte, dass das, was in einem Koalitionsvertrag angekündigt wird, tatsächlich politisch gewollt sei und umgesetzt würde, der könnte angesichts solcher vagen Formulierungen ausgerechnet in einer Digitalstrategie ernüchtert sein.[4] Nicht mehr an der Verabschiedung eines Beschäftigtendatenschutzgesetzes will sich die Regierung messen lassen, sondern nur noch daran, ob die bestehenden Gesetze zu mehr Rechtssicherheit beitragen. Fragt man Insider, ob an einem Beschäftigtendatenschutzgesetz ernsthaft gearbeitet wird, dann erhält man hinter vorgehaltener Hand eine abschlägige Antwort.

Offiziell erklärte das BMAS allerdings auf explizite Nachfrage noch im September 2022:

In Umsetzung des Koalitionsvertrages ist vorgesehen unter gemeinsamer Federführung von BMAS und BMI ein eigenständiges Beschäftigtendatenschutzgesetz zu schaffen. In einem ersten Schritt werden dazu gemeinsame Eckpunkte erarbeitet. Die sich daran anschließende Ausarbeitung eines Referentenentwurfs soll noch in der ersten Hälfte der Legislaturperiode erfolgen. Die Ergebnisse des Beirats zum Beschäftigtendatenschutz bilden eine wichtige Grundlage bei der inhaltlichen Gestaltung der Regelungen und finden bei der Erarbeitung der Eckpunkte sowie des Referentenentwurfes entsprechend Berücksichtigung. Vertreterinnen und Vertreter der Sozialpartner wurden bereits im Rahmen der Beiratsarbeit angehört. Bei der weiteren Ausarbeitung sowohl der Eckpunkte als auch des Referentenentwurfs wird das BMAS sowohl die Sozialpartner als auch weitere relevante Stakeholder einbeziehen.[5]

Demnach wäre mit einem Entwurf bis spätestens Oktober 2023 zu rechnen. Die Hoffnung auf ein Beschäftigtendatenschutzgesetz soll also noch nicht ganz beerdigt werden. Allerdings sind die Vorzeichen wenig ermutigend.

II. Der Beirat zum Beschäftigtendatenschutz

Hubertus Heil, Bundesarbeitsminister auch in der 19. schwarz-rot-regierten Legislaturperiode, hatte am 20.06.2020 einen „Beirat zum Beschäftigtendatenschutz" eingesetzt, der die Grundlage für ein Gesetz legen sollte. Schwarz-Rot hatte sich damals im Koalitionsvertrag auferlegt *zu prüfen, ob ein eigenständiges Gesetz zum Beschäftigtendatenschutz, das die Persönlichkeitsrechte der Beschäftigten am Arbeitsplatz schützt und Rechtssicherheit für den Arbeitgeber schafft,* sinnvoll und notwendig wäre. Um alle Aspekte zu berücksichtigen, wurde dieser Beirat tarifpartei- und disziplinübergreifend besetzt, und zwar mit kompetenten Vertreterinnen und Vertretern von Arbeitgebern und Arbeitnehmern, Wissenschaftlern, Praktikern, Datenschützern, Ethikern, Rechtsanwälten, Juristen und Informatikern. Die Leitung des Beirats wurde in prominente Hände gelegt – in die der früheren Bundesjustizministerin und Arbeitsrechtlerin Herta Däubler-Gmelin.[6]

Der Beirat führte – auch in der Coronazeit – eine Vielzahl von Beratungen und Anhörungen (u.a. mit Vertretern der Bundesvereinigung der Arbeitgeberverbände, des Deutschen Gewerkschaftsbunds, der Datenschutzkonferenz, der Datenethikkommission, mit betrieblichen Datenschutzbeauftragten, Betriebsräten und Unternehmensvertretern) durch. Sein Ergebnis ließ auf sich warten. Zuletzt war vorgesehen den Abschlussbericht noch in der 19. Legislaturperiode im Sommer 2021 abzuliefern. Daraus wurde nichts. Erst im Januar 2022, also schon in der 20. Legislaturperiode, wurde ein Kurzbericht veröffentlicht, der eine allgemeine Orientierung gibt, wohin es mit einem

Beschäftigtendatenschutzgesetz gehen könnte.[7] Die Entwürfe für einen über 100 Seiten umfangreichen Langbericht sahen nie das Licht der Öffentlichkeit. Der Grund: Die Arbeitgebervertreter verweigerten sich einer kontroversen Darstellung und verließen schließlich sang- und klanglos den Beirat. Rechtsanwalt Tim Wybitul, der regelmäßig Arbeitgeber vertritt, erklärte: „Ich kann nichts unterschreiben, was ich nicht später vor Gericht und vor meinen Mandanten gut vertreten kann." Angeblich habe es im Langbericht keine abweichenden Voten geben sollen. Dies kann nicht zutreffen. Selbst im Kurzbericht wird zwischen Beiratsmehrheit und -minderheit unterschieden. Dass sich die Arbeitgeberseite beschwerte, mit ihrer Meinung nicht hinreichend berücksichtigt zu werden, ist wenig überzeugend. Es war nämlich ausgerechnet die Arbeitgeberseite gewesen, die beim Beiratsstart zunächst für einen Konsensbericht plädiert hatte.[8]

Die Geschichte des Beirats zum Beschäftigtendatenschutz ist eine weitere traurige Episode einer never-ending Tragödie, die nun mit einem stillschweigenden Verzicht auf das in der 20. Legislatur angekündigte Gesetz ihre Fortsetzung finden könnte.

III. Das bisher unvollendete Gesetz

Diese Tragödie hat eine ca. 50-jährige Geschichte: 1971 sprach sich ein im Auftrag des Bundesministeriums des Innern erstelltes Expertengutachten zur Schaffung gesetzlicher Datenschutz-Grundlagen für eine spezifische Regelung für Beschäftigte aus.[9] Mit dem Volkszählungsurteil des Bundesverfassungsgerichts (BVerfG) 1983 wurde diese Forderung nach einem bereichsspezifischen Gesetz zusätzlich verfassungsrechtlich grundiert.[10] In späteren Entscheidungen bekräftigte das BVerfG, dass es Aufgabe des Rechts sei zu verhindern, dass sich im Privatrecht, wozu das Arbeitsrecht gehört, „für einen Vertragsteil die Selbstbestimmung in Fremdbestimmung verkehrt".[11] Die der Aussage zugrundeliegende Beschreibung eines Machtgefälles zwischen Vertragsparteien gilt ohne Einschränkungen für das Verhältnis zwischen Arbeitgeber und Arbeitnehmer.

Angesichts dieser verfassungsrechtlichen Vorgaben war es konsequent, dass seit der Volkszählungsentscheidung die Regierungsparteien in ihren Koalitionsabsprachen auf Bundesebene immer wieder ankündigten ein Beschäftigtendatenschutzgesetz[12] zu schaffen. Alle Versuche, ein solches Gesetz zu verabschieden, scheiterten aber am politischen Widerstand der Arbeitgeberseite.[13] Nur ein einziges Mal fand sich in einem Koalitionsvertrag keine Selbstverpflichtung zur Erarbeitung eines solchen Gesetzes – in der 2005 beginnenden 16. Legislaturperiode. Just in dieser Periode gab es in Deutschland derart viele Überwachungsskandale im Beschäftigtenbereich, dass sich die CDU-SPD-Regierung 2009 noch kurz vor der nächsten Bundestagswahl genötigt sah mit dem damaligen § 32 Bundesdatenschutzgesetz (BDSG) zumindest minimale Schutzvorschriften ins Gesetz aufzunehmen.[14] Die damals ergänzte (und seitdem ob ihrer Interpretierbarkeit immer wieder kritisierte) Regelung wurde, leicht modifiziert, nach der Umsetzung der Datenschutz-Grundverordnung (DSGVO) 2019 in den aktuell gültigen § 26 BDSG überführt.

Nicht nur auf nationaler, sondern auch auf europäischer Ebene blieben alle Versuche, den Persönlichkeitsschutz Beschäftigter zu verbessern, in ersten Ansätzen stecken. Eine von der EU-Kommission initiierte Konsultation zum Arbeitnehmerdatenschutzrecht in den Jahren 2001/2002 hatte keine weiteren Initiativen zur Folge. Ein Grund hierfür war wohl, dass selbst auf nationaler Ebene die EU-Mitgliedstaaten fast durchgängig keinen Regelungsbedarf oder – vielleicht wegen des Widerstands der Arbeitgeberseite – keine Einigungsmöglichkeit sahen.

Mit der seit 2009 geltenden europäischen Grundrechte-Charta (GRCh) werden sowohl ein Grundrecht auf Datenschutz (Art. 8) als auch umfassende Arbeitnehmerrechte auf oberster Regulierungsebene garantiert.[15] Zudem können weitere Grundrechte betroffen sein – sowohl der Beschäftigten[16] als auch der Unternehmen[17]. In der DSGVO wurde in Art. 88 ein allgemeiner rechtlicher Rahmen für die nationalen Gesetzgeber sowie für kollektivrechtliche Normen vorgegeben. Die eigentliche Normsetzung soll durch die Mitgliedstaaten erfolgen.[18] Der europäische Gesetzgeber will bisher keine die DSGVO präzisierende Regelung ausarbeiten.

Die politischen Ansagen sowohl in der 19.[19] als auch nun in der 20. Legislaturperiode des Bundestags waren und sind eigentlich klar. Dem entsprechen Forderungen aus Gewerkschaften[20], der arbeitsrechtlichen Praxis[21], dem institutionellen Datenschutz[22] und der Wissenschaft[23]. Die gesetzgeberische Zielsetzung ist ein umfassendes Gesetz zum Datenschutz für Beschäftigte. Kurz vor Ende der 19. Legislaturperiode verständigten sich CDU und SPD – ohne großes öffentliches Aufsehen – auf ein Betriebsrätemodernisierungsgesetz.[24] Darin wurden einige Datenschutzfragen geregelt, insbesondere die Mitbestimmungspflicht beim Einsatz künstlicher Intelligenz (§ 90 Abs. 1 Nr. 3 BetrVG) sowie die Klärung der unsäglichen Streitfrage zur Verantwortlichkeit des Betriebsrats für seine eigene Datenverarbeitung (§ 79a BetrVG).[25] Eine umfassende Regelung des Beschäftigtendatenschutzes erfolgte nicht.

Auch wenn die Begeisterung für ein umfassendes Gesetz in der Bundesregierung weiterhin wenig ausgeprägt scheint, könnte sich nun Druck auf europäischer Ebene aufbauen. Eine Vorlage des Verwaltungsgerichts (VG) Wiesbaden beim Europäischen Gerichtshof (EuGH) stellt diesem die Frage, ob der deutsche Gesetzgeber mit § 26 Abs. 1 S. 1 BDSG (bzw. mit dem inhaltlich identischen § 23 Abs. 1 S. 1 HDSIG) seiner Konkretisierungs- bzw. Spezifizierungspflicht nach Art. 88 DSGVO in Bezug auf den Beschäftigtendatenschutz nachgekommen ist, indem er einfach die europäische Regelung wiederholte.[26] In seinem Votum kommt der Generalanwalt beim EuGH zu dem Ergebnis, dass die deutschen Regelungen nicht mit EU-Recht vereinbar seien, da das Wiederholungsverbot[27] verletzt würde und im nationalen Recht keine spezifischeren Regelungen erlassen worden seien.[28] Solche spezifischeren Regelungen müssten gemäß Art. 88 Abs. 2 DSGVO „geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person" enthalten, was bei § 26 Abs. 1 S. 1 BDSG

nicht zuträfe.[29] Der EuGH folgt in der Regel dem Entscheidungsvorschlag des Generalanwalts. Wäre dies auch hier der Fall, dann wäre die Generalklausel des § 26 BDSG nicht mehr anwendbar[30]; die Gesetzgeber in Deutschland müssten wohl tätig werden.

Derweil verstärkt sich das Machtgefälle zwischen Arbeitgebern und deren Dienstleistern einerseits und den Beschäftigten und ihren Vertretungen andererseits durch immer komplexere Systeme und Verfahren, die zweckübergreifend und oft unternehmensübergreifend ausgeklügeltere intransparente Auswertungen über die Beschäftigten ermöglichen, ohne dass diesen adäquate Rechte zustehen.[31]

IV. Grundüberlegungen zum BeschDSG

Die eingangs geäußerte Hoffnung ist also nicht nur noch lebendig, sie ist auch höchst notwendig. Und daher muss man sich mit den möglichen und notwendigen Inhalten eines Beschäftigtendatenschutzgesetzes (BeschDSG) befassen.[32] Dem sollen einige grundsätzliche Erwägungen vorangestellt werden:

Es ist klar, dass ein BeschDSG einen Ausgleich zwischen den Grundrechten der Arbeitgeber und denen der Beschäftigten vornehmen muss. Beide Seiten sind – Ausnahme ist das öffentliche Dienstecht – als „private" Grundrechtsträger und als Vertragspartner in ihrer Autonomie zu achten. Bei dem Ausgleich muss berücksichtigt werden, dass sich der Arbeitgeber strukturell in einer stärkeren Position befindet, da er durch die Verfügungsmacht über die Produktionsmittel sowie durch seine ökonomische, juristische, informationstechnische und soziale Potenz den Beschäftigten überlegen ist. Die Rechte des Arbeitgebers werden gegenüber Beschäftigten durch ein umfassendes Direktionsrecht (§ 106 Abs. 1 GewO) umgesetzt. Zum Schutz vor dem strukturell überlegenen Vertragsteil hat ein BeschDSG individuelle Rechte für den Beschäftigten vorzusehen, wobei zwischen materiellen und prozessualen Rechten unterschieden werden kann. Ergänzend – auch durch das Grundgesetz abgesichert – stehen den Arbeitnehmern betriebsverfassungsrechtlich garantierte Kollektivrechte zu, die im BeschDSG in Bezug auf den Datenschutz konkretisiert werden könnten.

Bisher ist der Beschäftigtendatenschutz in Deutschland in § 26 BDSG sowie in spezifischen weiteren Gesetzen, etwa den Sozialgesetzbüchern (SGB), dem Arbeitssicherheitsgesetz (ASiG), dem Allgemeinen Gleichstellungsgesetz (AGG) und vielen weiteren – auch untergesetzlichen – Normen geregelt. Angesichts der bestehenden Komplexität ist es weder möglich noch wünschenswert diese Normen in ein BeschDSG zu integrieren, zumal sie dann aus ihren spezifischen Zusammenhängen herausgerissen würden. Wohl aber ist es geboten die allgemeinen Regeln, also insbesondere die zu allgemein gehaltenen Inhalte des § 26, aus dem BDSG herauszulösen und ein eigenes Gesetz zu schaffen. Ein Aufblähen des BDSG wäre wenig anwendungsfreundlich. Wenn auf die DSGVO oder das BDSG verwiesen werden kann sind Regelungen im BeschDSG zu vermeiden. Sinnvoll können aber Regelungen sein, in denen die Vorgaben des allgemeinen Datenschutzrechts konkretisiert werden, etwa zu Datenschutz-Folgenabschätzungen bei der Verarbeitung von Beschäftigtendaten (Art. 35 DSGVO), zu Datenschutzbeauftragten (Art. 37, 38 DSGVO), zu Abwägungen als Rechtsgrundlage (Art. 6 Abs. 1 lit. f DSGVO), zum Auskunftsrecht Beschäftigter (Art. 15 DSGVO), zu Betriebsvereinbarungen als Rechtsgrundlage (Art. 88 DSGVO), zur Zertifizierung von Verfahren (Art. 42 DSGVO) oder zu Aufgaben der Aufsichtsbehörden (vgl. Art. 58 Abs. 6 DSGVO).

Die kollektivrechtliche Seite des Beschäftigtendatenschutzes hat bisher vor allem im Betriebsverfassungsgesetz ihre Grundlage, etwa das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG. Da eine Modernisierung des Beschäftigtendatenschutzes auch eine kollektivrechtliche Seite haben muss, ist es naheliegend parallel das BetrVG und evtl. das Tarifrecht zu ändern, etwa indem zusätzliche Mitbestimmungsrechte eingeführt oder über den Datenschutz hinaus Klagerechte eingeräumt werden. Rein datenschutzrechtliche Festlegungen sollten im BeschDSG normiert werden. Wichtig ist in jedem Fall, dass die Verknüpfung der beiden Rechtsmaterien erkennbar ist.

Es ist im Arbeitsrecht noch weit verbreitet das Datenschutzrecht als eine separate Materie anzusehen und zu behandeln. Dies resultiert beispielsweise in der immer noch anzutreffenden Ansicht, dass in Mitbestimmungsprozessen keine Datenschutzfragen zu thematisieren seien. Entsprechende Herangehensweisen sind bzw. waren im Zivilrecht generell wie speziell im Verbraucher- und im Wettbewerbsrecht zu verzeichnen.[33] Sie ignorieren, dass alle bestehenden Regelungen Bestandteil eines einheitlichen Normgefüges sind, bei dem eine künstlich abschottende Sichtweise zwangsläufig zu Inkonsistenzen und Rechtsverkürzungen führen muss.

Das Beschäftigtendatenschutzrecht wird bisher vorrangig durch die Rechtsprechung konturiert, der des Bundesarbeitsgerichts (BAG) und der Arbeitsgerichte, zunehmend auch über Urteile des Europäischen Gerichtshofs (EuGH). Diese zurückblickende Konkretisierung des Datenschutzes über Einzelfälle erhöht nur bedingt die Rechtssicherheit bei den Beteiligten. Auch muss man konstatieren, dass es für bestimmte Anwendungsfälle, wie beispielsweise zur Videoüberwachung am Arbeitsplatz, eine jahrzehntelange, verfestigende Rechtsprechung gibt, für andere Fragestellungen jedoch keine, sehr wenige oder gar widersprüchliche Entscheidungen. Insbesondere für kleine und mittlere Unternehmen sowie bei Unternehmen ohne Mitbestimmung bestehen für Arbeitgeber und Arbeitnehmer daher viele Unwägbarkeiten bei der Rechtsanwendung. Absehbare technische, ökonomische und soziale Entwicklungen können in Gerichtsurteilen – anders als durch Entscheidungen des Gesetzgebers – nicht berücksichtigt werden. Ein BeschDSG muss dem Anspruch gerecht werden materiell sowie durch klar festgelegte Verfahren die Rechtssicherheit zu erhöhen. Es muss zugleich technologieoffen sein, um für absehbare Änderungen anwendbar zu sein ohne sinnvollen Fortschritt zu hindern. Bei der Festlegung der Regeln können bei der gerichtlichen Kasuistik mit ihren Einzelfallabwägungen Anleihen gemacht werden.

Es wird kontrovers diskutiert, was „spezifischere Vorschriften" i.S.v. Art. 88 Abs. 1 DSGVO sind, die über die Öffnungsklausel sowie in Kollektivvereinbarungen erlaubt sind. Unstreitig ist dabei, dass die DSGVO einen Mindeststandard festlegt, der nicht unterschritten werden darf; die Grenzen der DSGVO sind einzuhalten. Die Diskussion, inwieweit darüber hinausgehende Abweichungen – insbesondere nach unten – zulässig sind, hat eher akademischen Charakter.[34] Das Recht zur Spezifizierung eröffnet einen Ermessensspielraum, wobei bei der Konkretisierung die spezifischen Aspekte des Beschäftigungsverhältnisses ausschlaggebend sein müssen. Es besteht die Möglichkeit zusätzliche, strengere oder einschränkende, nationale Vorschriften vorzusehen.[35] Im Folgenden sollen einige wesentliche Regelungsaspekte eines BeschDSG dargestellt und erörtert werden.

V. Wesentliche Regelungsaspekte

a. Allgemeine Regelungen

Bisher wird der Anwendungsbereich des Beschäftigtendatenschutzes durch § 26 Abs. 8 BDSG in Verbindung mit § 5 BetrVG festgelegt. Erfasst werden Arbeitnehmer einschließlich Leiharbeitnehmer[36], Auszubildende, Rehabilitanden, Beschäftigte in Behindertenwerkstätten, Personen, die Freiwilligendienste oder Zivildienst leisten, Beamte und Richter des Bundes, Soldaten und insbesondere auch die aufgrund ihrer wirtschaftlichen Unselbstständigkeit als arbeitnehmerähnlich einzuordnenden Personen. Erfasst werden zudem Personen, die sich für ein Beschäftigungsverhältnis bewerben oder deren Beschäftigungsverhältnis beendet ist. Sinnvoll ist es die neue Kategorie der Crowdworker, also von Beschäftigten, die über das Internet Dienstleistungen für ein Unternehmen erbringen, als arbeitnehmerähnliches Beschäftigungsverhältnis zu präzisieren und von wirtschaftlich nicht abhängigen Soloselbstständigen abzugrenzen.[37]

Hinsichtlich der Wirksamkeit von Einwilligungen im Arbeitskontext macht § 26 Abs. 2 BDSG mit seiner Vermutungsregelung zur Freiwilligkeit schon heute eine präzisierende Vorgabe. Insofern sind beispielhafte Ergänzungen möglich.

b. Bewerbungssituation

Mehr und mehr Unternehmen stützen zumindest Teile ihrer Datenverarbeitung im Bewerbungsprozess auf die Einwilligung der sich Bewerbenden. Dies gilt beispielsweise für nicht im strengen Sinne erforderliche Fragen, für das Durchführen von Persönlichkeitstest und Gesundheitsuntersuchungen und für den Einsatz von digitalen Auswahlverfahren. Auch der Einsatz vermeintlicher künstlicher Intelligenz (KI), etwa durch Sprach- oder Mimikanalyse, soll häufig auf Einwilligungen basieren.[38] Ein aktuell von der EU-Kommission verfolgter Regelungsansatz sieht vor, dass besonders invasive Analyseverfahren nur eingeschränkt oder überhaupt nicht erlaubt sein sollen. Gemäß dem Kommissions-Vorschlag soll der Einsatz von KI bei der Einstellung und Auswahl von Personen, für Entscheidungen über Beförderung und Kündigung sowie für die Zuweisung, Überwachung oder Bewertung von Personen in Arbeitsvertragsverhältnissen als hochriskant (Art. 6 ff. i.V.m. Anhang III Nr. 4 Entwurf KI-Verordnung) eingestuft werden (s.u. VII.).[39]

Der Bewerbungsprozess ist bisher gesetzlich nicht näher geregelt. Die arbeitsgerichtliche Rechtsprechung erlaubt dem Arbeitgeber Fragen zu stellen, an deren Beantwortung er ein „berechtigtes, billigenswertes und schutzwürdiges Interesse" hat.[40] Eine Datenerhebung im Rahmen der Bewerbung muss – im Hinblick auf die angestrebte Stelle – „erforderlich" sein. Zudem gelten die europarechtlich determinierten, diskriminierungsrechtlichen Regelungen des AGG (§ 6 Abs. 1 S. 2 AGG). Es besteht ein „Recht auf Lüge".[41] Hinsichtlich einer Erhebung bei Dritten, etwa bei früheren Arbeitgebern oder im Internet (durch sog. Background-Checks)[42], muss – nicht zuletzt zur Vermeidung von Falschbewertungen – die Einbeziehung der Betroffenen gewährleistet sein. Im Interesse der Rechtsklarheit sollte die bisherige Rechtsprechung gesetzlich fixiert werden, auch im Interesse einer Eindeutigkeit hinsichtlich der Rechtsfolgen im Fall eines Verstoßes. Der Abgleich von Bewerbenden- und Beschäftigtendaten mit sog. Anti-Terror- oder Sanktionslisten bedarf in jedem Fall einer ausdrücklichen, für die Betroffenen transparenten Rechtsgrundlage, so dass eine Rechtsschutzmöglichkeit eröffnet wird. Auch dies ist gesetzlich klarzustellen.

Tests und Untersuchungen können als Einstellungsvoraussetzung erforderlich sein, um die körperliche und psychische Eignung für die konkret angestrebte Stelle festzustellen, etwa bei Tätigkeiten mit Drittgefährdungsmöglichkeit.[43] Solche Tests sind aber nur akzeptabel, wenn sie – was gesetzlich vorzugeben ist – von qualifiziertem Personal gemäß einem (z.B. durch Zertifizierung) validierten Verfahren durchgeführt werden. Hierzu gehört, dass – entsprechend der betriebsärztlichen Betreuung – nur die Ergebnisse der Tests und Untersuchungen, nicht aber die zumeist äußerst sensiblen erhobenen Daten dem Arbeitgeber bekannt werden.[44]

Es sollte ganz allgemein präzisiert werden, dass das durch die jeweilige Interessenslage gekennzeichnete Machtgefälle zwischen Bewerbenden und potenziellem Arbeitgeber eine freiwillige Einwilligung nicht ermöglicht, die Einwilligung als Rechtsgrundlage im Bewerbungsprozess also ausscheidet.

c. Verarbeitung während des Beschäftigungsverhältnisses

Angesichts der vielen unterschiedlichen Fallgestaltungen erscheint eine abschließende Listung der zulässigen Kontrollzwecke im Beschäftigungsverhältnis nicht möglich. Unbefriedigend ist aber auch die in § 26 Abs. 1 S. 1 BDSG enthaltene, auf Art. 88 Abs. 1 S. 1 DSGVO zurückgehende Generalklausel (s.o. III.). Es ist möglich und nötig typische konkretisierte Zwecke beispielhaft zu benennen, wodurch zugleich – bei entsprechender Dokumentation – eine Zweckdifferenzierung erreicht werden kann: Einhaltung gesetzlicher Verpflichtungen, Schutz des Eigentums und Vermögens des Arbeitgebers, Wahrung von Betriebsgeheimnissen, Optimierung von Arbeitsprozessen, Qualitätssicherung der Produktion, Aufdeckung von Straftaten und groben Pflichtverletzungen, Entgeltabrech-

nung, betriebliches Eingliederungsmanagement.[45]

Hinsichtlich der Art und der Intensität der Datenerhebung können gesetzlich relevante Kriterien benannt werden, die bei der Verhältnismäßigkeitsprüfung anzulegen sind, z.B. die zeitliche und räumliche Dimension von Kontrollen, die Sicherung von kontrollfreien Bereichen, Art und Anlass von Kontrollmaßnahmen, prozedurale Vorgaben, Transparenz gegenüber den Betroffenen. Als absolute Grenze sollte eine lückenlose technische Kontrolle am Arbeitsplatz, also eine Dauer- und Totalüberwachung, ausdrücklich ausgeschlossen werden.[46] Die Kriterien dafür, wann von einer solchen Dauer- und Totalüberwachung auszugehen ist, müssen klar definiert werden.

Zumindest für Daten, die alleine aus Gründen der Sicherstellung des ordnungsgemäßen Betriebs und zur Fehlerbehebung erhoben und weiterverarbeitet werden, sollte eine enge Zweckbindung bestehen. Dies betrifft insbesondere so genannte Protokolldaten (Logfiles), die sowohl die Administration als auch die Nutzung von Systemen automatisiert nachzeichnen. Eine Zweckänderung nach Art. 6 Abs. 4 DSGVO sollte ausdrücklich ausgeschlossen werden.

Ein außerdem regulierungsbedürftiger Sonderfall der Beschäftigtenkontrolle ist die im Homeoffice, da hier der räumliche, zeitliche und sozial-familiäre Intimbereich durch Arbeitgebervorgaben tangiert sein kann.[47] Insofern kann und muss die Einwilligung der Betroffenen von Relevanz sein.

d. Ausgewählte konkrete Kontrollanlässe und -maßnahmen

Heimliche Kontrollmaßnahmen des Arbeitgebers, die nur in begründeten Einzelfällen, also ausnahmsweise erlaubt sein können, sind von materiellen Voraussetzungen abhängig zu machen (z.B. zur Aufklärung von erheblichen Straftaten oder schweren Pflichtverletzungen).[48] Anlass für derartige Maßnahmen muss in jedem Fall ein zu dokumentierender konkreter hinreichender Verdacht sein. Im Interesse der Wahrung der Verhältnismäßigkeit ist ein eskalierendes Vorgehen zu prüfen. Die Maßnahmen bedürfen einer verfahrensmäßigen Einhegung. Diese kann darin bestehen, dass der betriebliche Datenschutzbeauftragte und der Betriebsrat einbezogen werden. Es ist klarzustellen, dass die Mitbestimmungsrechte durch einen datenschutzrechtlich normierten Erlaubnistatbestand nicht obsolet werden.

Im Rahmen des Arbeitsverhältnisses entstehen angesichts einer zunehmenden Digitalisierung im Bereich der Produktion, Kommunikation und Organisation oft zwangsläufig bzw. nebenbei beschäftigtenbezogene Daten. Hierbei kann es sich um sensitive i.S.v. Art. 9 DSGVO oder sonstige besondere schutzbedürftige Daten handeln. Deren Sekundärnutzung und die damit verbundene Zweckänderung, z.B. für Verhaltens- und Leistungskontrollen, muss auf das unbedingt erforderliche und verhältnismäßige Maß eingeschränkt werden. Sie muss in einem für die Beschäftigten transparenten und damit kalkulierbaren Verfahren erfolgen. Die Einbeziehung des Betriebsrats bei diesem Verfahren sollte gesetzlich vorgesehen werden; die konkrete Ausgestaltung in Form von Informations-, Kontroll- und Interventionsrechten kann Betriebsvereinbarungen überlassen werden (zur Mitbestimmung s.u. V.e.). Die Zweckänderung von besonders invasiv erhobenen Daten, etwa über Gefühle oder Gesundheitszustände, ist vollständig gesetzlich auszuschließen.

Arbeitgeber schalten bei ihrer Datenverarbeitung zunehmend Dritte ein, die Hard- und Software (z.B. beim Cloud-Computing) bereitstellen, aber auch weitergehende Dienstleistungen und Personal zum Einsatz bringen. Es ist gesetzlich sicherzustellen, dass hierbei der Arbeitgeber, etwa durch die Vertragsgestaltung mit dem Dienstleister, gewährleistet, dass sämtliche individuellen und kollektiven Rechte der Betroffenen bzw. des Betriebsrates wahrgenommen werden können.[49] Weiterhin muss gewährleistet werden, dass diese Dienstleister die erhobenen Daten nur für legitime und nicht für kommerzielle eigene Zwecke nutzen. Beispielsweise ist klarzustellen, dass die Nutzung von Beschäftigtendaten (Kundendaten) durch den Dienstleister zur Weiterentwicklung eines eigenen Produkts als kommerzielle Nutzung gilt und zu unterbleiben hat.

Insbesondere Arbeitgeber in Konzernverbünden strukturieren ihre Arbeitshierarchie häufig über eine sog. Matrix-Organisation. Diese dient in der Regel der gesellschaftsübergreifenden Projektarbeit und soll die disziplinarischen Zuständigkeiten auch über die Arbeitgebergrenzen hinweg innerhalb eines Mutterkonzerns sicherstellen, wozu ein berechtigtes Interesse des Arbeitgebers bestehen kann. Überschreiten die Konzernunternehmen hierbei reine Hilfsfunktionen und bestimmen dadurch Zwecke und Mittel der Datenverarbeitung, so besteht eine gemeinsame datenschutzrechtliche Verantwortung. Gesetzlich kann zumindest beispielhaft aufgeführt werden, wann in solchen Fällen ein berechtigtes Interesse des Arbeitgebers besteht und welche berechtigten Interessen von Beschäftigten der Verarbeitung entgegenstehen können. Der Arbeitgeber hat in diesen Fällen jedenfalls sicherzustellen, dass für die Beschäftigten transparent ist, welcher Konzernteil welche Aufgaben wahrnimmt. Werden hierbei Beschäftigtendaten des Arbeitgebers mit Daten anderer Konzernunternehmen verknüpft so sind, unbeschadet bestehender Mitbestimmungsrechte der Interessenvertretungen, durch explizit festzulegende und zu dokumentierende geeignete Maßnahmen die Beschäftigteninteressen sicherzustellen.

Die Verarbeitung sensitiver Daten gemäß Art. 9 DSGVO, insbesondere von Gesundheitsdaten, ist schon bisher weitgehend bereichsspezifisch geregelt.[50] In diesen Regelungen sind Anlass, Zweck, Umfang und Beteiligte der Datenverarbeitung zumeist rechtssicher festgelegt. Zudem besteht in § 26 Abs. 3 BDSG eine generalklauselhafte Regelung ohne praktische Relevanz. Da sie lediglich europarechtliche Vorgaben wiederholt, dürfte diese Regelung, ebenso wie § 26 Abs. 1 S. 1 BDSG, europarechtlich unzulässig und deshalb nicht anwendbar sein (s.o. III.). Die Notwendigkeit einer über die bereichsspezifischen Festlegungen hinausgehenden gesetzlichen Norm bedarf einer näheren Begründung, zumal Spezifizierungen des Art. 9 Abs. 2 lit. b DSGVO auch durch Kollektivvereinbarungen nach Art. 88 Abs. 1 DSGVO möglich sind. Jedenfalls sind zusätzliche Sicherungen vorzusehen.

Hinsichtlich der Eingriffsschwere ist die Verarbeitung von sensitiven Daten mit Verhaltens- und Leistungskontrollen oder mit dem Einsatz von KI-Verfahren vergleichbar. Es bietet sich an zumindest diese Art der Datenverarbeitung auch mitbestimmungspflichtig zu machen (s.u. weitergehend V.e.).

Der Einsatz von sog. künstlicher Intelligenz (KI) in Beschäftigungsverhältnissen nimmt stark zu, etwa in Bewerbungsverfahren, bei der Gefahrenvorsorge, beim Einsatz von sog. sozialen Medien oder im Rahmen der Produktion. Die Regelung des Art. 22 DSGVO, die die automatisierten Entscheidungen auch im Beschäftigungsverhältnis reguliert, greift vielmals zu kurz.[51] Im Fall einer Regulierung bedarf es zunächst einer möglichst präzisen Festlegung, welche Verfahren erfasst sein sollen. Angesichts des Umstands, dass die EU eine umfassende KI-Verordnung plant, die auch für Beschäftigungsverhältnisse gelten soll (s.o. V.b.), erscheint eine nationale materiell-rechtliche Vollregelung nicht erforderlich. Um zu vermeiden, dass sich eine entsprechende Praxis etabliert, sollte aber klargestellt werden, dass der Einsatz von KI allein auf Basis einer individuellen Einwilligung nicht statthaft ist. Eine Unterrichtungspflicht in Bezug auf KI wurde 2021 mit dem Betriebsrätemodernisierungsgesetz in den §§ 80 Abs. 3 S. 2, 90 Abs. 1 Nr. 3 BetrVG konkretisiert. Eine Mitbestimmungspflicht beim KI-Einsatz in Personalentscheidungen wurde in § 95 Abs. 2a BetrVG eingeführt.[52]

Die EU hat eine Whistleblower-Richtlinie[53] erlassen, die am 17.12.2021 in deutsches Recht hätte umgesetzt sein müssen. Nunmehr liegt ein Entwurf eines Hinweisgeberschutzgesetzes vor, der wohl hauptsächlich bei Beschäftigungsverhältnissen anzuwenden sein wird. Dieser in manchen Einzelfragen noch umstrittene Entwurf wird voraussichtlich in Bälde Gesetz.[54] Angesichts dessen scheint es nicht angebracht allgemeine Regelungen hierzu in ein BeschDSG zu integrieren. Es kann aber evtl. zusätzlich nötig sein, spezifisch arbeitsrechtliche Fragen, etwa zu einem Disziplinierungs- und Kündigungsschutz oder Aspekte zum Umfang der trotz gesetzlicher Vorgabe bestehenden Mitbestimmungsrechte bei der Ausgestaltung konkreter Hinweisgebersysteme in das Hinweisgeberschutzgesetz oder auch ins BeschDSG aufzunehmen.

e. Kollektivrechtliche Aspekte

Der Betriebsrat hat gemäß § 80 Abs. 1 Nr. 1 BetrVG die Aufgabe die Einhaltung der Arbeitnehmer schützenden Gesetze zu überwachen. Hierzu gehört die Überwachung der Beachtung des Datenschutzrechts. Dies wird in § 75 Abs. 2 S. 1 BetrVG bestärkt, wonach es dem Betriebsrat zukommt die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern. Diese Förderungsaufgabe kann dadurch verstärkt werden, dass dem Betriebsrat insofern gesetzlich explizit ein Initiativrecht zugestanden wird.

Durch das Betriebsrätemodernisierungsgesetz wurde in § 79a BetrVG klargestellt, dass die datenschutzrechtliche Verantwortlichkeit für die personenbezogene Verarbeitung durch den Betriebsrat beim Arbeitgeber verbleibt. Der unabhängige Betriebsrat hat mit dem Arbeitgeber zu kooperieren. Beispielhaft können die sich hieraus ergebenden Pflichten konkretisiert werden, etwa in Bezug auf die Erstellung des Verarbeitungsverzeichnisses nach Art. 30 DSGVO, die Umsetzung der Betroffenenrechte nach Art. 12 ff DSGVO oder die Erstellung eines Löschkonzepts für die beim Betriebsrat rechtmäßig verarbeiteten Daten. Hinsichtlich der Datenschutzkontrolle beim Betriebsrat ist vorstellbar, dass der Datenschutzbeauftragte hiermit ein Betriebsratsmitglied beauftragt.

Datenschutzbeauftragter und Betriebsrat verfolgen bzgl. der Verarbeitung von Beschäftigtendaten gleichgerichtete Aufgaben und Interessen. Um eine enge und gute Kooperation zu erleichtern, ist es sinnvoll, unabhängig von bestehenden Mitbestimmungsrechten nach § 99 BetrVG, die Einstellung und Abberufung von (internen wie externen) Datenschutzbeauftragten mitbestimmungspflichtig zu machen.[55] Bei der Beurteilung der gesetzlich geforderten fachlichen Kompetenz, zu der auch die Kompetenz gehört die Persönlichkeitsrechte der Beschäftigten zu wahren, ist die Erfahrung und Expertise des Betriebsrates von Bedeutung. Angesichts des erhöhten Kündigungsschutzes, den betriebliche Datenschutzbeauftragte genießen, ist es schon bei deren Bestellung von zentraler Bedeutung, dass diese Person das Vertrauen des Betriebsrats genießt und die Fähigkeit hat in datenschutzrechtlichen Konflikten im Betrieb zwischen Arbeitgeber und Arbeitnehmervertretung zu vermitteln.

Eine Erweiterung der Mitbestimmungspflicht bietet sich – in Erweiterung des § 87 Abs. 1 Nr. 6 BetrVG – generell für die Ausgestaltung und Konkretisierung des Beschäftigtendatenschutzes im Betrieb an. Es ist bisher oft unklar, inwieweit bei Verfahren, die zur Verhaltens- und Leistungskontrolle geeignet sind, Regelungen in einer Betriebsvereinbarung erlaubt und geboten sind (zu Verarbeitungszwecken, Zugriffsberechtigungen, Löschkonzepten, technisch-organisatorischen Maßnahmen, Betroffenenrechten).[56] Durch eine entsprechende Erweiterung kann diese Unsicherheit beseitigt und dem Auftrag in § 75 Abs. 2 S. 1 BetrVG eine prozessuale Grundlage gegeben werden.[57] Zudem sollte künftig gesetzlich gewährleistet werden, dass Betriebsräte bei der Erstellung einer Datenschutz-Folgenabschätzung für Beschäftigtendaten verarbeitende Systeme und Verfahren gemäß Art. 35 Abs. 9 DSGVO zwingend eingebunden werden.[58]

Der von Art. 88 DSGVO vorgesehene Abwägungsprozess kann über in Betriebsvereinbarungen fixierte angemessene Garantien gestaltet werden. Dies kann der Fall sein, wenn die Wahrung schutzwürdiger Betroffeneninteressen eine Verarbeitung zur Umsetzung berechtigter Interessen legitimieren soll (Art. 88 Abs. 1 S. 1 i.V.m. Art 6 Abs. 1 lit. f DSGVO), was auch im Fall der Verarbeitung sensitiver Daten relevant sein kann (Art. 9 Abs. 2 lit. b DSGVO). Bei Datentransfers in ein aus Datenschutzsicht unsicheres Drittland können dort geeignete Garantien geregelt werden, die z.B. ergänzend zu Standarddatenschutzklauseln oder Binding Corporate Rules (Art. 47 DSGVO) zur Anwendung kommen (Art. 46 DSGVO).

In der Praxis wird häufig darüber gestritten, ob der Betriebsrat einen Anspruch darauf hat, dass ihm die vom

verantwortlichen Arbeitgeber zu erstellenden datenschutzrechtlichen Dokumente, soweit sie die Verarbeitung von Beschäftigtendaten betreffen, gemäß § 80 Abs. 2 S. 2 BetrVG vorgelegt werden müssen. Zwecks Klarstellung der Rechtslage sollte festgehalten werden, dass dem Betriebsrat die relevanten Dokumente (u.a. Verarbeitungsverzeichnis gemäß Art. 30 DSGVO, Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO, Verträge zur Auftragsverarbeitung und zur gemeinsamen Verantwortlichkeit gemäß Art. 26, 28 DSGVO, Zertifizierungsunterlagen gemäß Art. 42 DSGVO, Verträge und Genehmigungen zur Drittauslandsübermittlung gemäß Art. 45 ff. DSGVO) bereitzustellen sind.

Die datenschutzrechtliche Expertise von Betriebsräten hat in den letzten Jahren zugenommen. In noch stärkerem Maße zugenommen hat aber die rechtliche und technische Komplexität von Informations- und Kommunikationssystemen. Diese entsteht durch erweiterte Funktionalität und Komplexität von Daten und Software, stärkere Vernetzung mit vielfältigen Schnittstellen, den Einsatz von nicht selbst betriebenen Systemen und generell durch die Einbindung externer IT-Dienstleister. Überschreiten Systeme eine bestimmte Komplexitätsschwelle, ist der Betriebsrat zur Wahrung seiner Aufgaben darauf angewiesen externen Sachverstand hinzuziehen. Die Bestimmung in § 80 Abs. 3 BetrVG zur Sicherstellung der erforderlichen sachverständigen Unterstützung sollte dadurch verbessert werden, dass die Hinzuziehung von Sachverständigen bei bestimmten Systemgestaltungen gesetzlich vermutet wird. Um den Anreiz zu erhöhen unabhängig geprüfte Verfahren einzusetzen, kann gesetzlich geregelt werden, dass im Fall einer Zertifizierung gemäß Art. 42 DSGVO die Rechtskonformität gesetzlich angenommen wird.[59]

f. Betroffenenrechte

Die Betroffenenrechte sind in den Art. 12 ff. DSGVO weitgehend abschließend reguliert. Zwar sind viele Aspekte in der Rechtsprechung und der Literatur umstritten. Eine Klärung dieser Streitfragen muss wegen des abschließenden Charakters der DSGVO jedoch weitgehend den Gerichten überlassen bleiben.[60] Eine Ausnahme hiervon besteht für Beschränkungen der Betroffenenrechte, wo über eine Öffnungsklausel Spielräume für nationale Regelungen bestehen (Art. 23 DSGVO). Insbesondere hinsichtlich des Schutzes der Rechte und Freiheiten anderer Personen (Art. 23 Abs. 1 lit. i DSGVO) bestehen arbeitsrechtliche Konkretisierungsmöglichkeiten. Es sollte klargestellt werden, dass Betriebs- und Geschäftsgeheimnisse dem individuellen Auskunftsersuchen nach Art. 15 DSGVO nicht entgegengehalten werden können.

Konkretisierungen sind auch hinsichtlich der Verfahren zur Inanspruchnahme der Betroffenenrechte vorstellbar, etwa zu Antwortfristen, zum Ablauf des Auskunftsverfahrens oder zum Technikeinsatz.

Große Unsicherheit besteht bisher hinsichtlich der Regelfristen für die Löschung personenbezogener Daten. Es gibt, etwa im Gesundheits-, im Steuer- und im Handelsrecht spezifische Regelungen, nicht aber für Standardprozesse in Beschäftigungsverhältnissen (Personalakte nach Beendigung des Beschäftigungsverhältnisses, Lohnnachweise, Zeugnisse und Bewertungen, Abmahnungen). Gesetzliche Vorgaben können hier Rechtssicherheit für alle Beteiligten schaffen. Auch sollten, möglicherweise mit Bezug auf DIN 66398, grundlegende Anforderungen an die Festlegung und Dokumentation von Regellöschfristen formuliert werden.

Besteht in einem Unternehmen ein Betriebsrat, haben die betroffenen Beschäftigten eine datenschutzrechtliche Interessenvertretung. Fehlt es hieran, so ist das Übergewicht der Arbeitgeberseite gegenüber den isolierten Beschäftigten höher. Dem kann durch kompensierende individuelle Rechte, z.B. solche, die ansonsten auch dem Betriebsrat zustehen, entgegengewirkt werden.[61]

g. Folgen rechtswidriger Datenverarbeitung und Rechtsdurchsetzung

Es ist oft streitig, inwieweit bei unzulässiger Datenerhebung und -speicherung ein Sachvortrags- oder ein Beweisverwertungsverbot im Rahmen von gerichtlichen Verfahren, etwa anlässlich einer Kündigung, besteht.[62] Hinsichtlich des gebotenen Interessenausgleichs der Beteiligten schafft eine gesetzliche Regelung mit Regelbeispielen, wofür die Rechtsprechung Anhaltspunkte liefern kann, mehr Klarheit. Zugleich lassen sich so die Anreize für eine unzulässige Datenverarbeitung verringern. Den Parteien sollte ausdrücklich in einer Betriebsvereinbarung die Möglichkeit der Vereinbarung von Verwertungsverboten eröffnet werden, auch bei der Missachtung von Mitbestimmungsrechten.

Das bestehende Abhängigkeitsverhältnis zum Arbeitgeber sowie Rechtsunsicherheiten können dazu führen, dass Beschäftigte vor einer Kontaktaufnahme mit der Aufsichtsbehörde zurückschrecken und eine gerichtliche Auseinandersetzung mit ihrem Arbeitgeber scheuen. Art. 80 DSGVO sieht vor, dass nicht nur die betroffene Person selbst, sondern Verbände im Verfahren oder Prozess auftreten können. Nach Art. 80 Abs. 1 DSGVO kann eine betroffene Person einen Verband insofern beauftragen, beispielsweise um ihr Beschwerderecht bei einer Aufsichtsbehörde auszuüben oder Ansprüche auf Information, Auskunft und Unterlassung gegen den Verantwortlichen geltend zu machen. Gemäß Art. 80 Abs. 2 DSGVO können Mitgliedstaaten ein von einem Auftrag durch Betroffene unabhängiges Verbandsklagerecht einführen – auch für Betriebsräte oder Gewerkschaften.[63] Damit kann ein Beitrag geleistet werden in Erweiterung der auf Verbraucher abzielenden europäischen Verbandsklagerichtlinie, die bis zum 25.12.2022 hätte umgesetzt werden müssen.[64] Mit kollektiven Rechtsdurchsetzungsmöglichkeiten können individuelle Rechtsverfahren vermieden und zugleich bestehende Vollzugsdefizite verringert werden. Dies erhöht die Rechtskonformität bei der Verarbeitung von Beschäftigtendaten und entlastet alle Beteiligten.

VI. Etablierung einer Beschäftigtendatenschutzkommission

Der Beirat zum Beschäftigtendatenschutz hat die Schaffung einer ständigen Beschäftigtendatenschutzkommission beim Bundesministerium für Arbeit und Soziales (BMAS) vorge-

schlagen, die Entwicklungen im Bereich des Beschäftigtendatenschutzes begleiten und abstrakte Regelungen für die Praxis konkretisieren soll. Die Beteiligung der Datenschutzaufsichtsbehörden und der Sozialpartner sollen hierbei sichergestellt werden. Das Gremium soll die Normgeber beraten und neue Instrumente in den Blick nehmen, etwa zur Entwicklung von Standards, Best-Practice-Ansätzen, Musterdokumenten, Audits und Prüfkriterien für Datenschutzzertifizierungen (vgl. Art. 42 Abs. 5 DSGVO). Ein solches Gremium kann dazu beitragen, dass angepasst an aktuelle technische Entwicklungen ein frühzeitiger Ausgleich zwischen Arbeitgeber- und Beschäftigteninteressen gesucht und gefunden wird und dass dieser Ausgleich nicht allein den Betriebsparteien und den Gerichten überlassen wird.[65]

VII. Schlussbemerkung

Die Geschichte des bisherigen Scheiterns eines Beschäftigtendatenschutzgesetzes und des Langberichts des dafür eingesetzten Beirats zeigt, dass eine Einigung zwischen Arbeitgeber- und Arbeitnehmervertretern bis heute nicht gelungen und auf kurze Sicht nicht absehbar ist. Die Arbeitgeberseite verweigert sich bisher einer zeitgemäßen Regulierung. Angesichts des hohen und zunehmenden Problempotentials darf dies nicht der Grund für die Politik sein sich den Regelungsnotwendigkeiten zu entziehen. Es ist gerade bei dieser Konstellation geboten zum Schutz der schwächeren Partei – der Beschäftigtenseite – gesetzliche Vorgaben zu machen. Dies hindert die Politik nicht den praktischen Bedürfnissen der Unternehmen hinsichtlich Rationalisierung der Datenverarbeitung und der Effektivierung von Organisation, Produktion und Verfahren durch Digitalisierung zu entsprechen. Die Politik hat in Deutschland aufgrund ihrer profunden Erfahrung im gesetzlichen Datenschutz die Möglichkeit EU-weit Standards zu setzen. Ein gutes Gesetz vermittelt der Arbeitgeberseite vielleicht die Einsicht, dass der Datenschutz der Beschäftigten letztlich auch in ihrem Interesse liegt und zu erhöhter Rechtssicherheit führt. Eine regulierte und interessenwahrende Datenverarbeitung erhöht die Zufriedenheit der Beschäftigten und dadurch deren Motivation, deren Zufriedenheit und letztlich deren Kreativität und Produktivität.

1 Dokumentiert in DANA 1/2022, 18 ff., hier 19.

2 BMAS veröffentlicht Ergebnisse des unabhängigen, interdisziplinären Beirats zum Beschäftigtendatenschutz, www.bmas.de 21.01.2022.

3 Digitalstrategie, Gemeinsam digitale Werte schöpfen, https://www.bmvi.de/SharedDocs/DE/Anlage/K/presse/063-digitalstrategie.pdf?__blob=publicationFile, S. 36 f.

4 Dazu DVD-PE 08.09.2022, Wissings Digitalstrategie ist ein wertloser Ankündigungskatalog, https://www.datenschutzverein.de/wp-content/uploads/2022/09/2022-09-Digitalstrategie.pdf; in diesem Heft, S. 248.

5 E-Mail des stellv. Pressesprechers des BMAS an die Autoren v. 27.09.2022.

6 Beirat Beschäftigtendatenschutzgesetz, DANA 3/2022, 183.

7 Abgedruckt in diesem Heft, S. 228.

8 Schulzki-Haddouti, Streit um Beschäftigten-Datenschutzgesetz, www.heise.de 13.05.2022, Kurzlink: https://heise.de/-7089189.

9 Steinmüller/Lutterbeck/Mallmann/Kolbe/Schneider, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministers des Innern, 1971, BT-Drs. VI/3826, S. 134 f., 155 ff.

10 BVerfG 15.12.1983 – 1 BvR 209/83 u.a., NJW 1984, 419 ff.

11 BVerfG 23.10.2006 – 1 BvR 2027/02, Rn. 33-36, JZ 2007, 577.

12 Damals noch: Arbeitnehmerdatenschutzgesetz.

13 Nachweise für die vielfachen Bestrebungen bei Seifert in Simitis, BDSG, 8. Aufl. 2016, § 32, Rn. 1.

14 Gesetz zur Änderung datenschutzrechtlicher Vorschriften v. 14.08.2009, BGBl. I S. 2814.

15 Art. 27 ff. GRCh: u.a. Rechte auf rechtzeitige Unterrichtung und Anhörung, auf kollektive Interessenverteidigung, auf gesunde, sichere und würdige Arbeitsbedingungen; dazu Weichert/Schuler, Besondere Probleme im Beschäftigtendatenschutz und Empfehlungen für ein Beschäftigtendatenschutzgesetz, 18.12.2020, www.netzwerk-datenschutzexpertise.de, S. 7 f.; Weichert NZA 2020, 1599.

16 Zu nennen ist insbesondere die freie Telekommunikation (Art. 10 GG, Art. 7 GRCh) und – wegen der zunehmenden Homeoffice-Tätigkeit – der Schutz der Wohnung (Art. 13 GG, Art. 7 GRCh).

17 Recht auf Eigentum, Berufsfreiheit, Unternehmensfreiheit, Art. 12, 14 GG, Art. 15-17 GRCh).

18 Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 2017, Teil 9 Rn. 6 (S. 134 f.).

19 Weichert/Schuler (En. 15), S. 5 f.

20 Statt vieler siehe Entwurf des DGB sowie Aufsatz von Wedde in diesem Heft, S. 224.

21 Rüdesheim AiB 2021, 30 ff.

22 Kelber/Blufarb ZRP 4/2022 Editorial. Datenschutzkonferenz, 04.05.2022, Die Zeit für ein Beschäftigtendatenschutzgesetz ist „Jetzt"! https://www.datenschutzkonferenz-online.de/media/en/Entschliessung_Forderungen_zum_Beschaeftigtendatenschutz.pdf.

23 Z.B Datenethikkommission, zit. in Weichert/Schuler (En. 15) S. 6 f.

24 G.v. 14.06.2021, BGBl. I S. 1762.

25 Rüdesheim AuR 2021, 345 f.; Kuß/Langenheim CR 2022, 235 ff.

26 VG Wiesbaden 21.12.2020 – 23 K 1360 / 20 WI.PV.

27 EuGH 07.02.1973 – C-39/72, Rn. 17; EuGH 10.10.1973 – C-34/73, Rn. 10, 11; Weichert in Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG, 2. Aufl., 2020, Einleitung Rn. 35a; Selmayr/Ehmann in Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Einführung Rn. 80.

28 EuGH-Generalanwalt Sanchez-Bordona 22.09.2022 – C-34/21, Rn. 58 ff.

29 EuGH-Generalanwalt Sanchez-Bordona 22.09.2022 – C-34/21, Rn. 69-75.

30 Schlussanträge des Generalanwalts v. 22.09.2022 – C-34/21.

31 Weichert/Schuler (En. 15); S. 10 ff.

32 Dazu schon – mit teilweise noch weitergehenden Vorschlägen – Weichert/Schuler (En. 15).

33 Weichert in Däubler/Wedde/Weichert/Sommer (En. 27), Einleitung UKlaG Rn. 3a ff., 9 ff.

34 BAG 27.05.1986 – 1 ABR 48/84, NJW 1987, 674 = MDR 1987, 83 = NZA 1986, 643 = BB 1986, 1087, 2333 = DB 1986, 2080, Rn. 97; Rüdesheim AuR 2021, 344; Klebe in Däubler/Klebe/Wedde, BetrVG, 18. Aufl., 2022, § 87 Rn. 195 m.w.N.

35 EuGH 28.04.2022 – C-319/20, NJW 2022, 1740 = NVwZ 2022, 945 = GRUR 2022, 920 = EuZW 2022, 522 = K&R 2022, 422 = afp 2022, 224, Rn. 57; EU-Generalanwalt

Sanchez-Bordona 22.09.2021 – C-34/21, Rn. 46.

36 Insofern muss festgelegt werden, dass deren Datenschutzrechte auch gegenüber dem ausleihenden Unternehmen gelten.

37 Däubler, Gläserne Belegschaften, 9. Aufl. 2021, Rn. 183d.

38 Greif/Kollmann ZAS 2021, 61 ff.; Hoffmann NZA 2022, 19 ff.

39 ErwGr 36 Entwurf KI-Verordnung

40 BAG 07.09.1995 – 8 AZR 828/93, NZA 1996, 637 = BB 1996, 217 = BB 1995, 1961 = DB 1996, 634.

41 Ständige Rechtsprechung seit BAG 05.12.1957 – 1 AZR 594/56, NJW 1958, 516 = MDR 1958, 372 = DB 1958, 227, 228, 282.

42 Däubler (En. 37), Rn. 211a.

43 So Vorgaben gemäß ArbSchG, ArbMedVV, SGB VII.

44 Schuler/Weichert, Die Datenverarbeitung des Betriebsarztes, www.netzwerk-datenschutzexpertise.de 22.09.2020, S. 8.

45 Däubler (En. 37), Rn. 394 ff.

46 BAG 27.03.2003 – 2 AZR 51/02, NJW 2003, 3436 = MDR 2004, 39 = NZA 2003, 1193 = BB 2003, 2578 = DB 2003, 2230 = JR 2004, 132.

47 Wedde AiB 2021, 24 f.; Leissler/Terharen ZAS 2022, 99 ff.; Müller, Homeoffice in der arbeitsrechtlichen Praxis, 2019.

48 EGMR (Große Kammer) 17.10.2019 - 1874/13, 8567/13, NJW 2020, 141 = NZA 2019, 1697 = AuR 2020, 131 (López Ribalda ua / Spanien).

49 Schuler/Weichert (En. 15), S. 14 f.

50 U.a. in SGB V, VII und IX, EFZG, ASiG, ArbSchG, ArbMedVV, IfSG, im Beamtenrecht; § 19 ff. GenDG.

51 Zu den allgemeinen datenschutzrechtlichen Anforderungen Datenschutzkonferenz, Hambacher Erklärung zur Künstlichen Intelligenz v. 03.04.2019.

52 Klebe CuA 10/2021, 16f.; Ruchhöft CuA 7-8/2021, 20 ff.; siehe auch Schröder/Höfers, Praxishandbuch Künstliche Intelligenz, 2022.

53 Richtlinie (EU) 2019/1937 v. 23.10.2019.

54 Dzida NZA 8/2022 Editorial; Gerdemann ZRP 2022, 98 ff.; Tölle ZRP 2022, 156 ff.

55 Rüdesheim AuR 2021, 347; Weichert/Schuler (En. 15) S. 25.

56 Dafür z.B. Holthusen RdA 2021, 28 ff.

57 Rüdesheim AuR 2021, 346 f.

58 Weichert/Schuler (En. 15) S. 20 f., 25 f.

59 Weichert/Schuler (En. 15), S. 21.

60 Zur Auskunft gemäß Art. 15 DSGVO Lembke/Fischels NZA 2022, 513 ff.

61 Weichert/Schuler (En. 15) S. 18 f.

62 Erfinger RdA 2021, 9 ff.; Rüdesheim AuR 2021, 347 f.

63 Rüdesheim AuR 2021, 348.

64 Oltmans NZA 16/2022 Editorial; Walter/Fischer K&R 2022, 32 ff.; Weichert/Schuler (En. 15) S. 26 f.

65 Weichert/Schuler (En. 15), S. 24.

Peter Wedde

Beschäftigtendatenschutz aus gewerkschaftlicher Sicht

Die Datenschutz-Grundverordnung (DSGVO) verzichtet darauf einheitliche europaweit gültige Regelungen zum Beschäftigtendatenschutz vorzugeben. Art. 88 DSGVO trägt zwar die Überschrift „Datenverarbeitung im Beschäftigungskontext“, beschränkt sich aber inhaltlich insbesondere darauf den Mitgliedsstaaten die Verantwortung für die Schaffung spezifischer gesetzlicher Regelungen zuzuweisen. Als mögliche Regelungsinhalte werden in Art. 88 Abs. 1 DSGVO Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags, des Managements, der Planung und der Organisation der Arbeit genannt, zudem zur Gleichheit und Diversität oder zur Gesundheit und Sicherheit am Arbeitsplatz sowie zum Schutz des Eigentums von Arbeitgebern und Kunden. Art. 88 Abs. 2 DSGVO gibt vor, dass Regelungen in den Mitgliedsstaaten insbesondere angemessene Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Personen umfassen sollen. Als spezifische Regelungsthemen werden die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb von Konzernstrukturen und Überwachungssysteme am Arbeitsplatz benannt.

In Deutschland wurde die durch die DSGVO eröffnete Möglichkeit zur Schaffung eines Beschäftigtendatenschutzgesetzes bisher nicht genutzt. Ein im Sommer 2020 vom Bundesminister für Arbeit und Soziales eingesetzter interdisziplinärer Expertenbeirat hat zwar anlässlich der Übergabe seines Berichts festgestellt, dass zentrale Elemente des Beschäftigtendatenschutzes einer wirksamen und rechtssicheren gesetzlichen Festlegung bedürfen.[1] Bundesarbeitsminister Hubertus Heil hat anschließend darauf hingewiesen, dass die neue Koalition in der aktuellen Legislatur Regelungen zum Beschäftigtendatenschutz schaffen will, um Rechtsklarheit für Arbeitgeber und Beschäftigte zu erreichen und die Persönlichkeitsrechte der Beschäftigten effektiv zu schützen.[2] Über den Arbeitsstand zu diesem Thema ist aber in der Öffentlichkeit bisher nichts bekannt. Damit setzt sich auf der politischen Ebene die „unendliche Geschichte“ fort, die sich bezüglich der Schaffung eines gesetzlichen Beschäftigtendatenschutzes in den letzten Jahrzehnten abgespielt hat.[3]

In der Arbeitswelt wurde und wird die Erforderlichkeit einer in sich geschlossenen Regelung zum Beschäftigtendatenschutz unterschiedlich eingeschätzt. Von Arbeitgeberseite wird ein solches Gesetz vielfach mit dem Argument abgelehnt, dass das geltende Datenschutzrecht ausreiche. Gewerkschaften, Betriebs- sowie Personalräte

und Beschäftigte halten hingegen einen gesetzlichen Beschäftigtendatenschutz für überfällig.

Wie ein Beschäftigtendatenschutzgesetz aussehen könnte, das den Schutz der Rechte von Beschäftigten und nicht Ansprüche der Arbeitgeber in den Vordergrund stellt, verdeutlicht der Entwurf für ein eigenständiges Beschäftigtendatenschutzgesetz (BeschDSG-E), den der Deutsche Gewerkschaftsbund (DGB) am 9. Februar 2022 vorgelegt hat.[4] Dieser Entwurf zielt insbesondere darauf ab Überwachungen von Beschäftigten zu verhindern, die heimlich, illegal oder unter Missachtung bestehender Mitbestimmungsrechte erfolgen. Zugleich soll das neue Gesetz Arbeitgebern und Beschäftigten bezüglich der Zulässigkeit von Verarbeitungen personenbezogener Daten eine Auseinandersetzung „auf Augenhöhe" ermöglichen.

Der BeschDSG-E bewegt sich mit seinen Regelungen zu relevanten Themen des Beschäftigtendatenschutzes innerhalb des allgemeinen gesetzlichen Rahmens, den DSGVO und Bundesdatenschutzgesetz (BDSG) vorgeben. Er wurde auf Grundlage eines von einem Wissenschaftler erarbeiteten Vorschlags zusammen mit Juristinnen und Juristen aus den DGB-Mitgliedsgewerkschaften entwickelt. Dem Konzept des BeschDSG-E liegt die Erkenntnis zugrunde, dass in der Arbeitswelt ein strukturelles Ungleichgewicht der Handlungs- und Reaktionsmöglichkeiten besteht, das Beschäftigte benachteiligt. Hiervon ausgehend verdeutlicht § 1 BeschDSG-E, dass mit den vorgeschlagenen Vorschriften vorrangig der Schutz der Interessen, Grundrechte und Grundfreiheiten der Beschäftigten einschließlich der Wahrung des Rechts auf informationelle Selbstbestimmung angestrebt wird. Verarbeitungen von Beschäftigtendaten durch Arbeitgeber sollen nur zulässig sein, wenn hierfür eine klare Erforderlichkeit besteht, etwa weil bestimmte Informationen für die Anbahnung, Durchführung oder Abwicklung von Beschäftigungsverhältnissen unumgänglich sind.

I. Anwendungsbereich

Das Gesetz kommt nach § 2 BeschDSG-E für die Verarbeitung von Beschäftigtendaten in der Anbahnungs- und Bewerbungsphase ebenso zur Anwendung wie während der Durchführung von Beschäftigungsverhältnissen oder nach deren Beendigung. Erfasst werden auch entsprechende Verarbeitungen durch Auftragsverarbeiter oder durch Dritte, die von Arbeitgebern ermöglicht oder veranlasst sind. Nicht in den Anwendungsbereich des Gesetzes fallen hingegen Verarbeitungen, die ausschließlich im Rahmen der Ausübung persönlicher oder familiärer Tätigkeit erfolgen, etwa das Festhalten von Erlebnissen aus dem Arbeitsalltag in einem privaten Tagebuch. Der gesetzliche Schutz soll nach § 2 Abs. 2 BeschDSG-E unterschiedslos für analoge wie für digitale Verarbeitungen bestehen.

Der in § 4 BeschDSG-E festgelegte räumliche Geltungsbereich bezieht Arbeitgeber aus dem öffentlichen wie aus dem nicht-öffentlichen Bereich unterschiedslos ein. Weit ist auch der in § 3 BeschDSG-E enthaltene persönliche Anwendungsbereich, der alle in der Begriffsbestimmung des § 5 Abs. 3 Ziff. 7 BeschDSG-E benannten Beschäftigten erfasst. Zu den Beschäftigten, die schon derzeit in § 26 Abs. 8 BDSG benannt sind, sollen künftig auch „allein tätige Selbstständige (‚Soloselbstständige')" gehören. Durch diese Erweiterung des Anwendungsbereichs sollen die personenbezogenen Daten von „Crowd-Workern" ebenso geschützt werden wie die von „selbstständigen" Beschäftigten im Logistikbereich. Grund für die Einbeziehung dieser Beschäftigtengruppen in den besonderen gesetzlichen Schutz ist der in den genannten Bereichen de facto bestehende Zwang Auftraggebern vielfältige Informationen zur Verfügung stellen zu müssen.

II. Grundsätze

Den materiellen Regelungen des BeschDSG-E sind (ähnlich wie in Art. 5 Abs. 1 DSGVO für die gesamte Verordnung) in Kapitel II des Entwurfs allgemeine Grundsätze vorangestellt, die bei jeder Verarbeitung von Beschäftigtendaten zu beachten sind. In § 6 Abs. 1 BeschDSG-E wird einleitend festgestellt, dass für die Verarbeitung von Beschäftigtendaten ein generelles „Verbot mit Erlaubnisvorbehalt" besteht. § 6 Abs. 3 BeschDSG-E macht klar, dass eine Verarbeitung von personenbezogenen Daten sowohl datenschutzrechtlich allgemein zulässig als auch für Zwecke des Beschäftigungsverhältnisses explizit erforderlich sein muss. Die Erforderlichkeit und die mit der Verarbeitung verfolgten Zwecke müssen Arbeitgeber in nachprüfbarer Weise festlegen und dokumentieren. Nach § 8 BeschDSG-E müssen diese weiterhin die Bewertungskriterien von durchgeführten Verhältnismäßigkeitsprüfungen dokumentieren.

Auf die Erhöhung der Transparenz zielt die in § 6 Abs. 4 BeschDSG-E verankerte Pflicht von Arbeitgebern zur Direkterhebung ab. Informationssammlungen über Beschäftigte im Internet oder aus anderen digitalen Quellen sind ausdrücklich unzulässig. Ausnahmen von diesem Verbot, etwa bezüglich der Bereitstellung von Informationen durch potentielle Beschäftigte in Bewerbungsportalen, sind in § 6 Abs. 6 BeschDSG-E benannt.

Die Voraussetzungen für das Bestehen einer Erforderlichkeit der Verarbeitung von personenbezogenen Daten für Zwecke des Beschäftigungsverhältnisses benennt § 9 BeschDSG-E, womit der „Besondere Teil B" mit den §§ 9 bis 40 eingeleitet wird. Arbeitgeber werden durch § 9 Abs. 2 BeschDSG-E beispielsweise dazu verpflichtet Beschäftigten und deren Interessenvertretungen auf Verlangen darzulegen, in welcher Form bei der Bewertung der Erforderlichkeit die allgemeinen Grundsätze in Art. 5 Abs. 1 DSGVO berücksichtigt werden. Durch § 11 BeschDSG-E wird die Zulässigkeit der Verarbeitung von Beschäftigtendaten innerhalb von Konzernstrukturen auf die Unternehmen beschränkt, in denen die Beschäftigten tätig sind.

Von herausragender Bedeutung für die Praxis ist die Regelung zur Zulässigkeit der Erteilung von Einwilligungen durch Beschäftigte in § 10 BeschDSG-E. Diese Norm benennt in ihrem ersten Absatz das Bestehen einer nachweisbaren Freiwilligkeit als Grundvoraussetzung für die Wirksamkeit einer Einwilligung. Abs. 3 nimmt zur Beurteilung der Freiwilligkeit den Regelungsgehalt auf, der derzeit in § 26 Abs. 2 BDSG enthalten ist. Durch § 10 Abs. 4 BeschDSG-E soll verhindert werden, dass potentielle Arbeitgeber von Bewerberinnen und Bewerbern auf der Basis von Einwilli-

gungen Information einfordern und erhalten, die außerhalb der datenschutzrechtlichen Erforderlichkeit stehen.

III. Bewerbungsphase

Der Datenverarbeitung in der Bewerbungsphase ist das Kapitel II des BeschDSG-E gewidmet. Die Vorschriften sollen sicherstellen, dass Arbeitgeber in dieser Phase nur solche Informationen erhalten, die für den Abschluss von Beschäftigungsverhältnissen erforderlich sind. Deshalb muss nach § 12 Abs. 3 BeschDSG-E von potentiellen Arbeitgebern der Grundsatz der Datenminimierung beachtet werden. Bedeutsam hierfür ist die in § 13 BeschDSG-E enthaltene Begrenzung des Fragerechts von Arbeitgebern. Diese Vorschrift nimmt Vorgaben der Rechtsprechung zum Fragerecht auf und stellt normativ klar, dass Bewerberinnen oder Bewerber Arbeitgebern nicht beliebige Informationen mitteilen müssen, sondern nur erforderliche. Durch die §§ 14 und 15 BeschDSG-E wird der Umgang mit personenbezogenen Informationen im Rahmen erforderlicher ärztlicher oder psychologischer Untersuchungen oder Testverfahren abgesteckt. Ausdrücklich verboten werden standardmäßig durchgeführte Drogen- oder Alkoholtests und psychologische Testverfahren, die derzeit von einzelnen Unternehmen ohne klare Rechtsgrundlage durchgeführt werden.

Durch die Regelungen zur Speicherbegrenzung und Datenlöschung in § 16 BeschDSG-E werden Arbeitgeber verpflichtet die personenbezogenen Daten erfolgloser Bewerbungen nach Ende des Verfahrens unverzüglich zu löschen. Wird eine Berücksichtigung von Bewerbungen in künftigen Verfahren in Aussicht gestellt, kann die Löschung auf Basis einer Einwilligung unterbleiben.

Durch die im BeschDSG-E enthaltenen Verarbeitungsregeln sollen die Verarbeitungsmöglichkeiten in der Bewerbungsphase insgesamt auf die aus objektiver Sicht notwendigen Informationen begrenzt werden. Zugleich erhöht sich durch die Übernahme von einschlägigen Vorgaben aus der Rechtsprechung sowohl für Arbeitgeber als auch für Bewerberinnen und Bewerber die Rechtssicherheit bezüglich der Zulässigkeit von Verarbeitungen in dieser Phase.

IV. Durchführung von Beschäftigungsverhältnissen

Im Mittelpunkt der vorgeschlagenen Regelungen zum Beschäftigtendatenschutz stehen die in Kapitel III enthaltenen Vorschriften für die Datenverarbeitung für Zwecke der Durchführung von Beschäftigungsverhältnissen. Mit dem Ziel der Wahrung der Interessen, Grundrechte und Grundfreiheiten der Beschäftigten legt § 17 Abs. 1 BeschDSG-E den Abschnitt einleitend fest, dass die Verarbeitungsbefugnisse von Arbeitgebern auf solche personenbezogenen Informationen beschränkt sind, die für die Durchführung der Beschäftigungsverhältnisse erforderlich sind. Zur Feststellung der Erforderlichkeit muss stets eine individuelle Interessenabwägung durchgeführt werden. Bei der Verarbeitung müssen nach Abs. 2 dieser Vorschrift die Verarbeitungsformen gewählt werden, die so wenig wie möglich in Rechte der Beschäftigten eingreifen. Flankiert wird diese grundsätzliche Vorgabe durch die in Abs. 3 enthaltene Verpflichtung zur Direkterhebung sowie durch die in Abs. 6 vorgegebene enge Zweckbindung.

Erwähnenswert ist § 17 Abs. 5 BeschDSG-E, der auf eine Begrenzung von „betrieblichen Hinweisgebersystemen" abzielt. Beschäftigte dürfen hiernach von Arbeitgebern nicht dazu aufgefordert werden personenbezogene Daten über mögliche Regel-, Vertrags- oder Gesetzesverstöße anderer Beschäftigter zu verarbeiten oder anderen Personen mitzuteilen. Diese Begrenzung schließt andere Konstrukte wie etwa die Benennung neutraler Personen oder Instanzen nicht aus.

Während laufender Beschäftigungsverhältnisse haben Arbeitgeber tatsächliche oder vermeintliche Erkenntnisinteressen, die zu Fragen an Beschäftigte führen können. Hinsichtlich des Fragerechts verweist § 18 BeschDSG-E auf die entsprechenden Regelungen in der Bewerbungsphase. Ergänzend hierzu wird durch § 19 Abs. 1 BeschDSG-E innerhalb laufender Beschäftigungsverhältnisse die Verarbeitung von Daten aus ärztlichen oder psychologischen Untersuchungen und Testverfahren nur zugelassen, wenn diese gesetzlich zwingend vorgeschrieben sind. Weitere Ausnahmen werden in Abs. 2 der Vorschrift für geplante dauerhafte Versetzungen erlaubt.

Die Verarbeitung von besonderen Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO verbindet sich mit der Offenbarung sensibler Informationen an Arbeitgeber, die aus Sicht der Beschäftigten besonders problematisch ist. Dies gilt insbesondere für Informationen zu Krankheiten, wenn diese Einfluss auf die berufliche Leistungsfähigkeit haben können. § 20 Abs. 1 BeschDSG-E lässt die Verarbeitung dieser Daten ausnahmsweise zu, wenn es hierfür eine freiwillige Einwilligung der Beschäftigten oder eine zwingende gesetzliche Verpflichtung gibt. Informationen zur politischen Ausrichtung, zur Gewerkschaftszugehörigkeit oder zur Religion dürfen zudem dann verarbeitet werden, wenn der Arbeitgeber eine Partei, eine Gewerkschaft oder eine Religionsgemeinschaft ist und wenn Beschäftigte einschlägige Aufgaben wahrnehmen müssen.

V. Kontrolle von Beschäftigten

Es ist unbestritten, dass Arbeitgeber bezüglich der Leistungserbringung und des beruflichen Verhaltens ihrer Beschäftigten über bestimmte Kontrollmöglichkeiten verfügen müssen. Der Zulässigkeit und Ausgestaltung derartiger Kontrollen ist Kapitel IV gewidmet, das in den §§ 21 bis 29 BeschDSG-E den Rahmen des Zulässigen benennt.

Bezogen auf erforderliche und damit zulässige Verhaltens- oder Leistungskontrollen legt § 21 Abs. 1 BeschDSG-E grundsätzlich fest, dass diese und die damit verfolgten Zwecke für betroffene Beschäftigte transparent und nachvollziehbar sein müssen. Verdeckte oder heimliche Überwachungsmaßnahmen werden ebenso für unzulässig erklärt wie anlasslose, zweckfreie oder dauerhafte Kontrollmaßnahmen.

§ 22 BeschDSG-E benennt Kontrollmöglichkeiten von Arbeitgebern zur Aufdeckung von Straftaten innerhalb von Beschäftigungsverhältnissen. Die Regelung ergänzt die aktuell in § 26 Abs. 1 S. 2 BDSG enthaltene Vorschrift durch eine frühzeitige Einbeziehung betroffener Beschäftigter in das Verfahren. § 22 Abs. 4 BeschDSG-E gibt vor,

dass die hierfür verwendeten personenbezogenen Daten datenschutzkonform erhoben wurden und dass sie überhaupt verarbeitet werden dürfen.

Die Zulässigkeit von Kontrollen mit Video- oder Audiosystemen sowie die Verwendung von vorhandenen Aufnahmefunktionen wird in den §§ 23 und 24 BeschDSG-E geregelt. Es werden Ausnahmesituationen benannt, in denen solche Verarbeitungen zulässig sein können. Gleiches gilt für die in § 25 BeschDSG-E zu findenden Begrenzungen der Verarbeitung von Beschäftigtendaten in „Cloud-Umgebungen" oder mit „KI-Anwendungen", die eine „zweckfreie Verarbeitung" sowie eine „allgemeine Vorratsdatenspeicherung" ausschließen.

Mit Blick auf aktuelle technische Entwicklungen besonders bedeutsam sind die in den §§ 26 und 27 BeschDSG-E enthaltenen Begrenzungen für die Verarbeitung von Standortdaten mittels integrierter Endgeräte sowie durch Ortungsverfahren. Diese Regelungen verpflichten Arbeitgeber zu einer engen Festlegung der verfolgten Zwecke und enthalten zugleich ein Verarbeitungsverbot für alle hierfür nicht benötigten Informationen. Die Vorschriften zielen auf die Herstellung eines angemessenen Interessenausgleichs. Dies gilt auch für § 28 Abs. 1 BeschDSG-E, der die Verarbeitung biometrischer Daten von Beschäftigten für den Regelfall untersagt. Ausnahmen von diesem Verbot sind nur für unumgängliche technische oder organisatorische Sicherheitsmaßnahmen vorgesehen. In diesem Rahmen anfallende Beschäftigtendaten müssen nach Erfüllung der festgelegten Zwecke von Arbeitgebern unverzüglich gelöscht werden.

Von großer praktischer Relevanz sind die Regelungen zum Ausschluss datenschutzwidriger Verarbeitungen und zu einem hieraus resultierenden Verwertungsverbot in § 29 BeschDSG-E. Verarbeitungen von Beschäftigtendaten, die gegen gesetzliche Vorschriften, gegen Regelungen in Kollektivvereinbarungen oder gegen kollektivrechtliche Beteiligungsrechte verstoßen, sind hiernach unzulässig. Diese Regelung bewirkt zulasten von Arbeitgebern ein normatives „Sachvortragsverwertungsverbot".

VI. Beendigung von Beschäftigungsverhältnissen

Durch § 30 BeschDSG-E wird in Kapitel V bezüglich der „Beendigung von Beschäftigungsverhältnissen" festgelegt, dass Beschäftigtendaten nach Ende einer Tätigkeit nur weiterverarbeitet werden dürfen, wenn gesetzliche oder kollektivrechtliche Verpflichtungen dies zwingend erforderlich machen. Mit Blick auf Art. 20 DSGVO werden Arbeitgeber durch § 31 BeschDSG-E verpflichtet ausscheidenden Beschäftigten nutzerspezifische Daten zur Verfügung zu stellen. Hierzu können etwa Daten gehören, die in einem individuell „angelernten" Spracherkennungssystem enthalten sind, aber auch für individuelle Arbeitserleichterung geschriebene Makros oder Apps. Der Anspruch entfällt, wenn durch eine entsprechende Übergabe Geschäftsgeheimnisse der Arbeitgeber offenbart würden.

VII. Einzelregelungen

Die abschließenden Kapitel VI und VII BeschDSG-E enthalten Regelungen zu Auskunftspflichten von Arbeitgebern gegenüber Beschäftigten in § 32 BeschDSG-E, ein Verbandsklagerecht für Gewerkschaften zur gerichtlichen Geltendmachung von Rechten für Beschäftigte in § 34 BeschDSG-E und eine Möglichkeit zur Gewinnabschöpfung in § 37 BeschDSG-E, die erfolgen kann, wenn Arbeitgeber in vorsätzlicher oder grob fahrlässiger Art und Weise mit einer unzulässigen Verarbeitung von Beschäftigtendaten Profite erzielen.

VIII. Fazit

Der DGB-Entwurf für ein BeschDSG stellt den Schutz der Interessen, Grundrechte und Grundfreiheiten in den Vordergrund. Diesen Schutzzielen müssen sich berechtigte Verarbeitungsinteressen der Arbeitgeber unterordnen. Ein solcher Schutzvorrang ist im Bereich des Arbeits- und Sozialrechts nicht unüblich und zielt darauf das bestehende Machtgefälle zu verringern. Insoweit handelt es sich nicht um einen neuen Regelungsansatz, sondern um die Übernahme des allgemeinen arbeitsrechtlichen Schutzkonzepts, das der Tatsache Rechnung trägt, dass Beschäftigte gegenüber Arbeitgebern nur über begrenzte Handlungsmöglichkeiten verfügen.

Die im BeschDSG-E vorgeschlagenen Regelungen lassen erforderliche Verarbeitungen, die Arbeitgeber für Zwecke der Anbahnung, Durchführung oder Beendigung von Beschäftigungsfeldes durchführen müssen, im notwendigen Maß zu. Insoweit werden deren Handlungsmöglichkeiten nicht ungebührlich eingeschränkt. Zugleich schafft der BeschDSG-E für Arbeitgeber wie für Beschäftigte Rechtsklarheit bezüglich zulässiger oder unzulässiger Verarbeitungen. Damit reduziert sich nicht nur der Aufwand, sondern auch die Zahl von innerbetrieblichen oder gerichtlichen Auseinandersetzungen zu diesem Thema. Schon deshalb ist zu hoffen, dass der Vorschlag des DGB den gesetzgeberischen Prozess für die Schaffung eines Beschäftigtendatenschutzgesetzes voranbringt.

1 Vgl. „Bericht des unabhängigen, interdisziplinären Beirats zum Beschäftigtendatenschutz, Januar 2022", S. 6 (abrufbar unter https://www.bmas.de/SharedDocs/Downloads/DE/Arbeitsrecht/ergebnisse-beirat-beschaeftigtendatenschutz.pdf.

2 Vgl. Pressemitteilung des Bundesministeriums für Arbeit und Soziales vom 17.1.2022 (abrufbar unter https://www.bmas.de/DE/Service/Presse/Meldungen/2022/bmas-veroeffentlicht-ergebnisse-des-beirats-zum-beschaeftigtendatenschutz.html).

3 Vgl. hierzu Wedde CuA 2/2022, S. 28.

4 Vgl. hierzu Piel in CuA 3/2022, S. 31. Der DGB-Gesetzentwurf ist abrufbar unter https://www.dgb.de/uber-uns/dgb-heute/recht/++co++d8c37b52-88e2-11ec-acce-001a4a160123.

Bericht des unabhängigen, interdisziplinären Beirats zum Beschäftigtendatenschutz

Einberufung des Beirats durch das Bundesministerium für Arbeit und Soziales

Mit der Einberufung des interdisziplinären Beirats zum Beschäftigtendatenschutz hat das Bundesministerium für Arbeit und Soziales den Auftrag aus dem Koalitionsvertrag der 19. Legislaturperiode umgesetzt zu prüfen, ob ein eigenständiges Gesetz zum Beschäftigtendatenschutz, das die Persönlichkeitsrechte der Beschäftigten am Arbeitsplatz schützt und Rechtssicherheit für den Arbeitgeber schafft, erlassen werden sollte (Koalitionsvertrag zwischen CDU, CSU und SPD vom 7. Februar 2018 für die 19. Legislaturperiode, Zeilen 6086 ff.).

Der Beirat nahm seine Arbeit unter Leitung der ehemaligen Bundesjustizministerin Prof. Dr. Herta Däubler-Gmelin im Juni 2020 auf. In regelmäßigen Sitzungen erörterten die Beiratsmitglieder die datenschutzrechtlichen Anforderungen einer sich schnell verändernden technologiegetriebenen Arbeitswelt. Im Zentrum der Beratungen standen juristische Fragen des Beschäftigtendatenschutzes, zugleich wurden die ethischen, wirtschaftlichen und technologischen Perspektiven betrachtet.

Die Mitglieder des Beirats kommen aus den Bereichen der Arbeits- und Organisationspsychologie, der Aufsichtsbehörden, der betrieblichen Praxis, der Ethik, der Informatik und der Rechtswissenschaft. Die diskutierten Themen reichten von den Grenzen der Kontrolle und Überwachung von Beschäftigten über die Frage des zulässigen Umfangs der Informationsbeschaffung über Bewerberinnen und Bewerber bis hin zum Einsatz sog. People Analytics Software im Bereich der Personalarbeit.

In die Beratungen, die pandemiebedingt hauptsächlich virtuell stattfanden, wurde ein breites Spektrum externer Expertise einbezogen. Allen voran brachten der Deutsche Gewerkschaftsbund und die Bundesvereinigung der Deutschen Arbeitgeberverbände wichtige Beiträge in die Diskussion ein. Ebenso wurden Vertreterinnen und Vertreter der Datenschutzkonferenz und der Datenethikkommission angehört. Aus der Praxis in den Betrieben berichteten interne und externe Datenschutzbeauftragte, Betriebsräte sowie Unternehmerinnen und Unternehmer. Der Beirat erhielt zudem Anregungen von Expertinnen und Experten aus dem Bereich Technologie, wie Prof. Dr. Katharina Zweig von der TU Kaiserslautern und Prof. Dr. Hannes Federrath von der Universität Hamburg, sowie aus der Zivilgesellschaft durch Matthias Spielkamp, Mitgründer und Geschäftsführer von AlgorithmWatch.

Der Beirat diskutierte und arbeitete unabhängig von der Einflussnahme Dritter.

Am 17. Januar 2022 übergab der Beirat für den Beschäftigtendatenschutz zum Abschluss seiner Tätigkeit die nachfolgenden Thesen und Empfehlungen zur Fortentwicklung des Beschäftigtendatenschutzes an den Bundesminister für Arbeit und Soziales, Hubertus Heil.

Thesen und Empfehlungen der Expertenkommission beim Bundesministerium für Arbeit und Soziales zur Fortentwicklung des Beschäftigtendatenschutzes

I. Tiefgreifende Veränderungen der Arbeitswelt durch die Digitalisierung

Seit einigen Jahren führt die fortschreitende Digitalisierung in Betrieben und Verwaltungen zu tiefgreifenden Veränderungen der Arbeitswelt. Dieser Prozess wird sich in den kommenden Jahren noch beschleunigen.

Datenbasierte Anwendungen prägen mittlerweile den Arbeitsalltag der meisten Beschäftigten. Die dynamische Entwicklung der neuen Informations- und Kommunikationstechnologien sorgt dafür, dass in den Betrieben und Verwaltungen immer mehr und immer detailliertere Datensätze entstehen, die – verbunden mit neuen Möglichkeiten ihrer Verknüpfung und Auswertung – Chancen für eine effizientere und menschengerechte Gestaltung der Arbeitsorganisation bieten. Zugleich ermöglichen diese Daten aber auch eine zunehmende Leistungsverdichtung sowie eine intensivere Kontrolle und Überwachung bis hin zu einer Durchleuchtung der Beschäftigten. Für beide Seiten – für die Beschäftigten wie für die Arbeitgeber – kann diese Entwicklung demnach einerseits klare Vorteile mit sich bringen: Arbeit kann durch digitale Unterstützung einfacher und weniger belastend sowie effizienter und kostengünstiger organisiert werden. Andererseits birgt die digitale Transformation für die Beschäftigten aber auch erhebliche Risiken, insbesondere im Hinblick auf ihre Persönlichkeitsrechte: Die feinkörnige Steuerung betrieblicher Prozesse lässt vielfach entsprechend detaillierte, auf die einzelnen Beschäftigten bezogene Datensätze entstehen, wodurch das Risiko einer immer umfassenderen Transparenz und Überwachung von Leistung und Verhalten der Arbeitnehmerinnen und Arbeitnehmer zunimmt. Es gilt den „Gläsernen Beschäftigten" zu verhindern.

Neue algorithmenbasierte Entscheidungsunterstützungssysteme ermöglichen zudem auf der Grundlage der erhobenen Daten Analysen bzw. Vorhersagen, aus denen sich tatsächliche oder vermeintliche Erkenntnisse zum Verhalten oder zu persönlichen Merkmalen von Beschäftigten ergeben. In der Bewerbungsphase kann dies dazu dienen die Eignung bzw. die Leistungspotenziale von Bewerberinnen und Bewerbern zu ermitteln sowie (vermeintliche) Defizite zu identifizieren. Während des Beschäftigungsverhältnisses kann darüber hinaus die Erfüllung der übertragenen Aufgaben detailliert bewertet

werden. Solche Systeme und Verfahren können auf der einen Seite zur Schaffung sachgerechterer Entscheidungen beitragen, auf der anderen Seite aber auch die Gefahr der Stärkung bestehender Vorurteile und der Schaffung neuer, intransparenter Diskriminierungen hervorrufen.

II. Fairer Ausgleich zwischen Beschäftigten- und Arbeitgeberinteressen

Der Beirat ist der Überzeugung, dass es immer wichtiger wird das Spannungsverhältnis zwischen den durch die Menschenwürde und den grundrechtlich geschützten Persönlichkeitsrechten und Interessen der Beschäftigten sowie den ebenfalls grundrechtlich geschützten Rechten und Interessen der Arbeitgeber durch ausgewogene Vorgaben zu regeln, um den verbindlich vorgegebenen Schutz der Beschäftigten durch ein wirksames Datenschutzrecht zu gewährleisten und auch bei einer weiterhin dynamisch fortschreitenden Digitalisierung der Arbeitswelt einen fairen Interessenausgleich herbeizuführen. Hierbei können Vereinbarungen der Arbeitgeber mit Betriebsräten eine besondere Rolle spielen.[1]

Bei der Bewältigung dieser Herausforderung ist es wesentlich die grundrechtlich geschützten Persönlichkeitsrechte der Beschäftigten und insbesondere deren Grundrecht auf informationelle Selbstbestimmung abzusichern. Dabei erfordert ein wirksamer Datenschutz klare und rechtssichere Regelungen, damit die Beschäftigten sich der Persönlichkeitsrechte bewusst sind und ihre Rechte geltend machen sowie Arbeitgeber ihre datenschutzrechtlichen Verpflichtungen erkennen können.

Zugleich stellt der Beirat fest, dass die Arbeitgeberseite bei der Verarbeitung von Beschäftigtendaten ebenfalls berechtigte, grundrechtlich geschützte Rechte und Interessen hat. Deshalb sind die Grundrechtspositionen der Beschäftigten und der Arbeitgeber in einen angemessenen Ausgleich zu bringen. Arbeitgeber und Beschäftigte sollten beim Umgang mit Beschäftigtendaten durch ein bundesweit einheitliches, rechtlich verbindliches und verlässliches Regelwerk rechtssicher einschätzen können, welche Entscheidungen und Maßnahmen bei der Verarbeitung von Beschäftigtendaten zulässig und welche unzulässig sind.

III. Gewährleistung der Grund- und Freiheitsrechte durch nationales, europäisches und internationales Beschäftigtendatenschutzrecht

Das Grundrecht auf informationelle Selbstbestimmung, das vom Bundesverfassungsgericht in seinem wegweisenden Volkszählungsurteil aus dem Jahr 1983 als Weiterentwicklung des Persönlichkeitsschutzes im Hinblick auf die Risiken zunehmender Datenverarbeitungsprozesse anerkannt worden ist, bildet als Ausprägung des untrennbar mit der Menschenwürde verbundenen Persönlichkeitsschutzes das grundrechtliche Fundament des Beschäftigtendatenschutzes in Deutschland. Der Beschäftigtendatenschutz mobilisiert den Grundrechtsschutz wesentlich über die Schutzpflichtdimension des Grundrechts auf informationelle Selbstbestimmung, die den Staat dazu anhält den grundrechtlichen Wertungen auch in Beschäftigungsverhältnissen mit privaten Arbeitgebern Geltung zu verschaffen.

Auf europäischer Ebene sind die Vorgaben der Charta der Grundrechte der Europäischen Union (GRCh) und der Datenschutz-Grundverordnung (DSGVO) maßgebend:

Art. 7 GRCh garantiert den Schutz der Privatsphäre. Art. 8 GRCh gewährleistet den grundrechtlichen Schutz personenbezogener Daten und etabliert damit das europäische Datenschutzgrundrecht, das zusätzlich durch Art. 16 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) geschützt wird. Die DSGVO als zentrales unionsrechtliches Rahmenwerk gilt auch für den Beschäftigtendatenschutz, enthält selbst allerdings nur rudimentäre auf diesen Bereich zugeschnittene Regelungen und überlässt es mit der Öffnungsklausel in Art. 88 DSGVO den Mitgliedstaaten durch Rechtsvorschriften und Kollektivverträge „spezifischere Vorschriften" für den Datenschutz im Beschäftigungskontext zu schaffen. Auf internationaler Ebene wird zudem mit Art. 8 der Europäischen Menschenrechtskonvention (EMRK) der Wert des Persönlichkeitsschutzes als „Recht auf Achtung des Privat- und Familienlebens" hervorgehoben, das sich auch auf die Rechtsbeziehungen zwischen Privaten auswirkt.

Der deutsche Gesetzgeber hat mit § 26 BDSG die ihm durch das europäische Recht eröffnete Möglichkeit zu spezifischeren Regelungen genutzt. Allerdings erlaubt § 26 BDSG vielfach keine treffsicheren Aussagen über die Zulässigkeit konkreter Verarbeitungen von Beschäftigtendaten im Einzelfall, sondern beschränkt sich im Wesentlichen auf generalklauselartige Regelungen. Als Instrument zur Sicherung von Menschenwürde, Grund- und Freiheitsrechten ist ein rechtssicherer und dadurch wirksamer Datenschutz im Beschäftigungskontext gerade im digitalen Zeitalter aber unverzichtbar. In diesem Sinne hatte sich der Gesetzgeber weitergehende Regelungen des Beschäftigtendatenschutzes seinerzeit ausdrücklich vorbehalten (BT-Drs. 18/11325, S. 97).

Die legitimen Interessen des Arbeitgebers an einer Verarbeitung von Beschäftigtendaten finden ihre rechtliche Grundlage insbesondere in der Gewährleistung seiner unternehmerischen Freiheit, im Schutz seiner Rechtsgüter – und dabei vor allem seines Eigentums – sowie in seinen Pflichten aus dem Arbeitsschutzrecht. Eine Abwägung und einen fairen Ausgleich zwischen den durch die Menschenwürde und weiteren grundrechtlich geschützten Rechten und Interessen der Arbeitnehmerseite und den grundrechtlich geschützten Rechten und Interessen der Arbeitgeberseite durchzuführen ist vornehmlich Sache des Gesetzgebers. Durch konkretisierende Regelungen kann erreicht werden, dass die rechtsverbindliche Klärung der Frage, welche Datenverarbeitungen im Beschäftigungsverhältnis für welche spezifischen Zwecke und unter welchen Voraussetzungen erforderlich sind, nicht mehr nur Gegenstand der Einzelfallkasuistik der Arbeitsgerichtsbarkeit ist.

IV. Leitgedanken einer spezifischen Regelung des Beschäftigtendatenschutzes

Die Anpassung und zukunftsfähige Weiterentwicklung des bestehenden

Beschäftigtendatenschutzrechts durch den Gesetzgeber an die Veränderungen der Arbeitswelt sollten sich in Ausfüllung seines verfassungs- und europarechtlichen Handlungsrahmens nach Auffassung des Beirats an folgenden Leitgedanken orientieren:

- verhältnismäßiger Ausgleich der beiderseitigen Grundrechte unter besonderer Beachtung des Schutzes der Menschenwürde der Beschäftigten,
- wirksamer Grundrechtsschutz und Rechtssicherheit für alle Beteiligten,
- Technologieneutralität und Technikoffenheit der Regelungen aufgrund der Dynamik der technischen Veränderungen,
- Transparenz für die betroffenen Beschäftigten und die Betriebsräte über die vom Arbeitgeber im Zusammenhang mit der Verarbeitung von Beschäftigtendaten verwendeten Einrichtungen und Programme,
- Gewährleistung einer wirksamen Rechtsdurchsetzung,
- auch bei der Weiterentwicklung des Beschäftigtendatenschutzrechts Beachtung der Verhältnismäßigkeit aller Maßnahmen nach Risikoabschätzung. Für neue Beschäftigungsformen, die im Zuge der digitalen Transformation der Arbeitswelt entstehen, empfiehlt der Beirat im Rahmen der durch Art. 88 DSGVO eröffneten Möglichkeit einer Spezifizierung des Beschäftigtendatenschutzes europarechtskonforme Nachjustierungen vorzunehmen.

V. Instrumente für die Weiterentwicklung des Beschäftigtendatenschutzrechts

Die zentralen Elemente eines wirksamen und rechtssicheren Beschäftigtendatenschutzes bedürfen der gesetzlichen Festlegung. Soweit die bereits vorhandenen Regelungen in der gegenwärtigen Fassung des § 26 BDSG aufgrund ihrer Interpretationsbedürftigkeit zum Schutz vor eingriffsintensiven Datenverarbeitungen in der digitalisierten Arbeitswelt nicht ausreichen, sind ausgewogene konkretisierende gesetzliche Regelungen für alle Beteiligten geboten. Daneben können untergesetzliche Regelungen wie Rechtsverordnungen und Kollektivverträge, aber auch neuartige Instrumente einen integralen Bestandteil eines wirksamen und rechtssicheren Beschäftigtendatenschutzes bilden. Als weitere spezifisch datenschutzrechtliche Instrumente sind die Erarbeitung von Verhaltensregeln (Codes of Conduct) im Sinne der Art. 40 f. DSGVO oder die Zertifizierung nach Art. 42 f. DSGVO empfehlenswert.

Bei der Fortentwicklung des Beschäftigtendatenschutzes sollten somit alle dem Staat und den privaten Akteuren zur Verfügung stehenden Instrumente einschließlich der Selbstregulierung in den Blick genommen werden:

- Wesentlich ist das Instrument einer gesetzlichen Regelung als ureigene Handlungsoption des Staates. Hierdurch kann die Grenzziehung zwischen rechtlich zulässigen und rechtlich unzulässigen Datenverarbeitungen für alle Beteiligten erkennbar verbindlich festgelegt werden.
- Untergesetzliche Instrumente können – auf der Grundlage angemessener gesetzlicher Ermächtigungen – dazu beitragen der für die Praxis wichtigen Grenzziehung zwischen dem rechtlich Zulässigen und Unzulässigen im konkreten Einzelfall deutlichere Konturen zu verleihen.

VI. Materielle und prozedurale Elemente zur Konkretisierung des geltenden Rechts

Zur Rechtfertigung der Verarbeitung von Beschäftigtendaten stehen gesetzliche Erlaubnistatbestände, die Einwilligung und Kollektivvereinbarungen zur Verfügung.

1. Konkretisierung der Erforderlichkeit bei gesetzlicher Verarbeitungserlaubnis

Im Hinblick auf diejenigen Rechtsgrundlagen aus der DSGVO und dem BDSG, die an das Merkmal der Erforderlichkeit anknüpfen, erachtet der Beirat Konkretisierungen des Schutzes der Persönlichkeitsrechte der Beschäftigten sowohl durch materiellrechtliche Grenzziehungen als auch durch prozedurale Elemente für sinnvoll.

Zum Datenerhebungsrecht („Fragerecht") des Arbeitgebers in der Bewerbungsphase hat sich über Jahrzehnte hinweg eine reichhaltige Einzelfallkasuistik, auch zu Einstellungstests und Einstellungsuntersuchungen, herausgebildet. Um ein möglichst hohes Maß an Wirksamkeit und Rechtssicherheit sowie an Einheitlichkeit im Beschäftigtendatenschutz zu erreichen, empfiehlt der Beirat relevante und typisierbare Fallkonstellationen in Gesetzesrecht zu überführen, sofern dies angesichts der Vielgestaltigkeit und Dynamik der Fallpraxis sachgerecht ist.

Soweit es um die Durchführung des Beschäftigungsverhältnisses geht, ist es für den Gesetzgeber zwar nicht leistbar jede denkbare Fallkonstellation in einen konkreten Tatbestand zu fassen. Dennoch sollten – wo möglich und angemessen – die wesentlichen Interessenabwägungen im Rahmen von neu zu schaffenden, spezifischen und normenklaren Vorschriften durch den Gesetzgeber selbst vorgenommen werden. Daneben empfiehlt der Beirat die gesetzliche Verankerung von insbesondere an Art. 5 DSGVO orientierten Parametern für die Prüfung der Erforderlichkeit, die vor allem die Art, den Umfang, die Intensität und die Umstände der Verarbeitung von Beschäftigtendaten berücksichtigen.

Des Weiteren muss sich der Leitgedanke der Transparenz von Kontroll- und Überwachungsmaßnahmen grundsätzlich auch im Kontext der Verhinderung und Aufdeckung von Straftaten bewähren. Die Mehrheit des Beirats ist der Auffassung, dass verdeckte Maßnahmen höchstens in Ausnahmefällen als ultima ratio zur Aufdeckung von Straftaten, nicht aber zur Aufklärung von sonstigen schweren Pflichtverletzungen grundsätzlich möglich sein sollten. Eine Minderheit des Beirats sieht verdeckte Maßnahmen in Ausnahmefällen als ultima ratio auch zur Verhinderung und Aufdeckung von schweren Pflichtverletzungen als zulässig an. Eine andere Minderheit lehnt verdeckte Maßnahmen ausnahmslos ab. Der Beirat empfiehlt in jedem Fall eine gesetzliche Klarstellung.

Erfolgen verdeckte Maßnahmen, muss die Kontrolle der Rechtmäßigkeit ex ante durch eine Einbeziehung von betrieblichen oder außerbetrieblichen Akteuren sichergestellt sein. Weiterhin müssen ex post die Transparenz des Verfahrens und die Information der Betroffenen gewährleistet sein.

Im Hinblick auf den Sonderfall des anlasslosen Abgleichs von Beschäftigtendaten mit Terrorismus- und Sanktionslisten hält die Mehrheit des Beirats einen solchen Abgleich allenfalls bei Schaffung einer spezifischen Rechtsgrundlage für zulässig. Eine Minderheit des Beirats hält die bestehenden rechtlichen Regelungen für die Legitimation derartiger Abgleiche dagegen für ausreichend.

2. Anforderungen an die Einwilligung als Ausdruck der Datensouveränität im Beschäftigungsverhältnis

Die Einwilligung ist Ausdruck des Rechts auf informationelle Selbstbestimmung. Insoweit gehört es zur Datensouveränität eines jeden Einzelnen frei und selbstbestimmt über die eigenen Daten verfügen zu können. Unter welchen Voraussetzungen die Einwilligung eine wirksame Rechtsgrundlage darstellen kann, ist in der DSGVO geregelt.

Die Einwilligung steht nach der DSGVO grundsätzlich gleichrangig neben anderen Erlaubnistatbeständen. Dabei ist die Freiwilligkeit der Einwilligung von zentraler Bedeutung. Wegen des im Beschäftigungsverhältnis grundsätzlich bestehenden Über-/Unterordnungsverhältnisses kann nach Ansicht der Mehrheit des Beirats von einer solchen Freiwilligkeit regelmäßig nur beim Vorliegen besonderer Umstände ausgegangen werden. Dies ist zum Beispiel der Fall, wenn die Beschäftigten mit der Einwilligung eigene Interessen oder im Verhältnis zum Arbeitgeber gleichgelagerte Interessen verfolgen.

Im Bewerbungsverfahren kann von einer Freiwilligkeit der Einwilligung der Bewerberinnen und Bewerber regelmäßig nicht ausgegangen werden. In dieser Situation bietet es sich an die in § 26 Abs. 2 Satz 1 BDSG bereits enthaltenen Regelungen zur Freiwilligkeit der Einwilligung zu ergänzen, um hierdurch mehr Rechtssicherheit zu schaffen. So sollten Regelbeispiele der Zulässigkeit bzw. der Unzulässigkeit einer Einwilligung sowohl für das Bewerbungsverfahren als auch für das Beschäftigungsverhältnis formuliert werden, um für beide Seiten die Rechtssicherheit zu erhöhen. Darüber hinaus bietet es sich nach Ansicht der Mehrheit des Beirats in Ergänzung des bestehenden Rechts an zu verdeutlichen, dass die Erreichung eines wirtschaftlichen Vorteils grundsätzlich nicht zu einem „Abkaufen“ der Einwilligung führen darf, damit Beschäftigtendaten nicht zu einer erwerblichen „Ware“ werden.

3. Bedingungen für Betriebsvereinbarungen als sachnahes Regelungsinstrument

Um das Ziel eines fairen Ausgleichs der Interessen zu erreichen, können die Betriebsparteien aktiv die beschäftigtendatenbezogenen Handlungsfelder adressieren und zu diesem Zweck Betriebsvereinbarungen abschließen. Die Mehrheit des Beirats ist der Auffassung, dass der verstärkte Einsatz von Betriebsvereinbarungen allerdings nur dann zu einem wirksameren Beschäftigtendatenschutz führen kann, wenn die Betriebsräte durch flankierende Regelungen im Betriebsverfassungsgesetz besser dazu befähigt werden ihrer Aufgabe gerecht zu werden die Persönlichkeitsrechte der Beschäftigten zu schützen. Eine Minderheit des Beirats befürwortet demgegenüber einen stärkeren Einsatz von Betriebsvereinbarungen generell als sachnahes Regelungsinstrument und setzt hierfür auch auf Anreize für die Arbeitgeberseite.

4. Datenschutzrechtliche Anforderungen an den Einsatz Künstlicher Intelligenz im Beschäftigungsverhältnis

Künstliche Intelligenz ist die nächste Stufe einer durch den technologischen Fortschritt getriebenen Digitalisierung und verdient deshalb eine eigenständige Betrachtung. Dabei versteht der Beirat unter Künstlicher Intelligenz nicht nur selbstlernende Systeme, sondern auch solche algorithmischen Systeme, deren Funktion und Wirkung aufgrund ihrer hohen Komplexität allenfalls für Expertinnen und Experten nachvollziehbar sind.

Der Beirat empfiehlt nachdrücklich den Einsatz von Künstlicher Intelligenz im Beschäftigtenkontext gesetzlich zu regeln. Hierbei sollte sich der Gesetzgeber an den sieben datenschutzrechtlichen Anforderungen an den KI-Einsatz, die die Hambacher Erklärung der Datenschutzkonferenz (DSK) formuliert hat, als wichtige Anregungen auch für die Regelung des Einsatzes von Künstlicher Intelligenz in Beschäftigungsverhältnissen orientieren. Darüber hinaus ist die Rechtsentwicklung auf der europäischen Ebene im Auge zu behalten.

VII. Spezifische Rechte der Betroffenen im Beschäftigungskontext

1. Konkretisierung der Betroffenenrechte

Rechtsstreitigkeiten vor den Gerichten und Diskussionen in der Literatur zeigen, dass im Hinblick auf die Rechte der betroffenen Personen bzw. die Pflichten des Verantwortlichen nach der DSGVO erhebliche Unsicherheiten und Unklarheiten bestehen. Die Umsetzung der Betroffenenrechte sollte im Kontext spezifischer Rechtsgrundlagen für typische Verarbeitungssituationen im Beschäftigtenverhältnis konkretisiert werden. Dabei ist der Auskunftsanspruch eines Beschäftigten als ein wesentliches Mittel zur Herstellung von Transparenz anzusehen, soweit er nicht sachfremd geltend gemacht wird.

2. Regelung von Sachvortrags- und Beweisverwertungsverboten

Die gesetzliche Normierung eines Verwertungsverbots für rechtswidrig verarbeitete Beschäftigtendaten in gerichtlichen Verfahren wurde im Beirat insbesondere vor dem Hintergrund der Prozessgrundrechte kontrovers diskutiert. Nach Auffassung der Mehrheit der Beiratsmitglieder sollte der Beschäftigtendatenschutz in Betrieben mit Betriebsrat dadurch effektiviert werden, dass den Betriebsparteien ausdrücklich die Möglichkeit eröffnet wird wirksame Verwertungsverbote in Betriebsvereinbarungen aufzunehmen. Ergänzend spricht sich die Mehrheit des Beirats im Hinblick auf den Beschäftigtendatenschutz für die gesetzliche Normierung eines Sachvortrags- und Beweisverwertungsverbots unter Nennung der Kriterien für eine gerichtliche Prüfung aus. Eine Minderheit des Beirats lehnt solche Regelungen als einen nicht sachgerech-

ten Eingriff in die freie richterliche Beweiswürdigung ab.

VIII. Ergänzende Regelungen im Betriebsverfassungsrecht im Interesse des Beschäftigtendatenschutzes

Betriebsräte spielen beim Beschäftigtendatenschutz eine zentrale Rolle: Sie haben die betriebsverfassungsrechtliche Aufgabe die Rechte und damit auch die Persönlichkeitsrechte der Beschäftigten zu schützen und zu fördern. Um dieser Aufgabe auch bei der fortschreitenden Digitalisierung der Arbeitswelt nachkommen zu können, bedarf es nach Auffassung der Mehrheit der Beiratsmitglieder ergänzender Regelungen im Betriebsverfassungsgesetz, wie zum Beispiel der Erweiterung der Mitbestimmungsrechte, bezogen auf den Beschäftigtendatenschutz, und der Erleichterung der Hinzuziehung von externen Sachverständigen. Eine Minderheit des Beirats lehnt demgegenüber eine Erweiterung von Mitbestimmungsrechten und insbesondere auch die Erstreckung der Mitbestimmung auf die Bestellung von Datenschutzbeauftragten als systemfremd und den Zielen des Datenschutzes hinderlich ab.

IX. Verbesserung der Rechtsdurchsetzung

Die Mehrheit des Beirats spricht sich für die Notwendigkeit einer Verstärkung der Möglichkeit zur Rechtsdurchsetzung aus und plädiert daher für eine verbesserte Rechtsstellung von Betriebsräten und Gewerkschaften im Rahmen des gerichtlichen Rechtsschutzes. Eine Minderheit des Beirats sieht hierfür dagegen keinen Regelungsbedarf.

Im Übrigen empfiehlt der Beirat einstimmig eine Stärkung der Durchsetzungsbefugnisse der Aufsichtsbehörden und der Unabhängigkeit der betrieblichen Datenschutzbeauftragten.

X. Datenschutzaufsichtsbehörden als Garanten eines wirksamen und rechtssicheren Beschäftigtendatenschutzes

Der Beirat ist der Auffassung, dass die Überwachung durch die Datenschutzaufsichtsbehörden wesentlich zu einem wirksamen und rechtssicheren Beschäftigtendatenschutz beiträgt.

Damit Verstöße gegen den Beschäftigtendatenschutz möglichst von vornherein vermieden bzw. frühzeitig aufgedeckt werden können, empfiehlt der Beirat die personelle Verstärkung der Aufsichtsbehörden. Diese Verstärkung soll es den Aufsichtsbehörden erleichtern auch eine ergänzende und unterstützende Beratung zu übernehmen.

XI. Errichtung einer Beschäftigtendatenschutzkommission und eines ständigen Sekretariats des AK Beschäftigtendatenschutz bei der DSK

Als Ergänzung zu einem eigenständigen Beschäftigtendatenschutzgesetz schlägt der Beirat die Schaffung von zwei neuen Gremien vor, die die fortlaufenden technischen und sonstigen relevanten Entwicklungen im Bereich des Beschäftigtendatenschutzes begleiten und abstrakte Regelungen für die Praxis konkretisieren sollen:

- eine ständige Beschäftigtendatenschutzkommission beim BMAS und
- ein ständiges Sekretariat des Arbeitskreises Beschäftigtendatenschutz der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz).

Die Beteiligung der Sozialpartner und die Unabhängigkeit der Datenschutzaufsichtsbehörden ist hierbei sicherzustellen.

Zu den Aufgaben dieser Gremien kann neben der Beratung des Gesetz- und Verordnungsgebers auch gehören sonstige Instrumente in den Blick zu nehmen, beispielsweise die Unterstützung von Best-Practice-Ansätzen, Veröffentlichung von Musterdokumenten, Selbstaudits zur regelmäßigen Bestandsaufnahme des Datenschutzniveaus und in Bezug auf Verarbeitungssysteme im Beschäftigungskontext die Bereitstellung von Prüfkriterien für die Auswahl und für einen datenschutzkonformen Einsatz sowie Hilfestellungen für ihre Entwicklung nach dem Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO). Dabei sind die besonderen Bedürfnisse von kleinen und mittleren Unternehmen zu berücksichtigen.

XII. Empfehlungen für Unternehmen ohne Betriebsrat und für neue Beschäftigungsformen

Der Beirat empfiehlt zur wirksamen Umsetzung und Durchsetzung des Beschäftigtendatenschutzes in Betrieben ohne Betriebsrat Handlungsempfehlungen für die datenschutzrechtlich Verantwortlichen zu erstellen, beispielsweise durch die zu schaffende Beschäftigtendatenschutzkommission beim BMAS.

Mit Blick auf datenbasierte Geschäftsmodelle und neue Beschäftigungsformen, etwa in der Plattformökonomie, ist der Gesetzgeber aufgerufen spezifische Regelungen zum Beschäftigtendatenschutz für diese Bereiche zu schaffen und für deren Umsetzung zu sorgen.

Der o.g. Beiratsbericht ist im Internet herunterladbar unter:
https://www.bmas.de/SharedDocs/Downloads/DE/Arbeitsrecht/ergebnisse-beirat-beschaeftigtendatenschutz.pdf

Mitglieder des Beirats
(Stand: 17. Januar 2022):

Prof. Dr. Herta Däubler-Gmelin (Vorsitzende) Rechtsanwältin, Bundesjustizministerin a. D.

Prof. Dr. Anne Riechert Professorin für Datenschutzrecht und Recht in der Informationsverarbeitung an der Frankfurt University of Applied Sciences; Wissenschaftliche Leiterin der Stiftung Datenschutz

Dir. u. Prof. Dr. Beate Beermann Vizepräsidentin der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin

Benedikt Rüdesheim, LL. M. Rechtsanwalt bei dka Rechtsanwälte, Fachanwalt für Arbeitsrecht

Marit Hansen Landesbeauftragte für Datenschutz Schleswig-Holstein, Diplom-Informatikerin

Prof. Dr. Judith Simon Professorin für Ethik in der Informationstechnologie an der Universität Hamburg

Prof. Ulrich Kelber Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

Prof. Dr. Prof. h.c. Jürgen Taeger Rechtsanwalt, Of Counsel bei DLA Piper LLP; zuvor Professor für Bürgerliches

Recht, Handels- und Wirtschafts- sowie Rechtsinformatik an der Carl von Ossietzky Universität Oldenburg
Thomas Koczelnik Ehemaliger Vorsitzender des Konzernbetriebsrats der Deutschen Post DHL Group
Prof. Dr. Peter Wedde Professor für Arbeitsrecht und Recht der Informationsgesellschaft an der Frankfurt University of Applied Sciences; Wissenschaftlicher Leiter der d+a consulting GbR in Wiesbaden
Prof. Dr. Rüdiger Krause Inhaber des Lehrstuhls für Bürgerliches Recht und Arbeitsrecht an der Georg-August-Universität Göttingen

1 Thesen und Empfehlungen, die Betriebsräte betreffen, gelten entsprechend für Personalräte, Mitarbeitervertretungen und Sprecherausschüsse.

Hajo Köppen*

Datenschutz-Tätigkeitsberichte – eine Fundgrube auch für Beschäftigtenvertretungen

Datenschutzvorschriften sind für juristische Laien meist schwer durchschaubar. Hilfe im Paragrafendschungel des Datenschutzrechts bieten die Tätigkeitsberichte der staatlichen Datenschützer – besonders wenn es um die praktische, auch technische Umsetzung geht. Für Betriebs- und Personalräte bieten die Berichte interessanten Lesestoff und praxisbezogene Beispiele zum Beschäftigtendatenschutz in Unternehmen und Behörden.

1972 erster Tätigkeitsbericht des Landesdatenschutzbeauftragten in Hessen

„Bis zum 31. März jeden Jahres, erstmals zum 31. März 1972, hat der Datenschutzbeauftragte dem Landtag und dem Ministerpräsidenten einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen." Mit diesem Auftrag im ersten Datenschutzgesetz der Welt, dem Hessischen Datenschutzgesetz von 1970, wurde die Tradition der Tätigkeitsberichte der Datenschutzbeauftragten begründet. Diese Berichtspflicht gilt inzwischen für alle staatlichen Datenschutzwächter – den Bundes- und die Landesdatenschutzbeauftragten – die seit dem ersten Bericht in Hessen über 600 Tätigkeitsberichte veröffentlicht haben. Die Berichte beschreiben eine Vielzahl in der behördlichen und betrieblichen Praxis auftretende Datenschutzprobleme und bieten an Hand von Praxisbeispielen rechtliche Hinweise genauso an wie hilfreiche Tipps für die konkrete Umsetzung des Datenschutzes.

Seit dem 25. Mai 2018 gilt die Europäische Datenschutz-Grundverordnung (DSGVO). Gem. Art. 59 DSGVO (Tätigkeitsbericht) hat jede Aufsichtsbehörde einen Jahresbericht über ihre Tätigkeit zu erstellen, der auch eine Liste der Arten der gemeldeten Verstöße und der Arten der getroffenen Maßnahmen nach Art. 58 Abs. 2 DSGVO (Befugnisse der Aufsichtsbehörden) enthalten kann. Die Tätigkeitsberichte müssen dem nationalen Parlament, der Regierung und anderen nach dem Recht der Mitgliedstaaten bestimmten Behörden übermittelt werden. Sie müssen ferner der Öffentlichkeit zugänglich gemacht werden.

Diesem Auftrag folgend werden von den 16 Landesdatenschutzbeauftragten, dem Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) und dem Bundesdatenschutzbeauftragten jedes Jahr insgesamt 18 Tätigkeitsberichte veröffentlicht.

Recherchehilfe zaftda.de

18 Tätigkeitsberichte mit insgesamt einigen hundert Seiten jährlich; das spricht für eine zeitintensive Recherche. Abhilfe und Zeitersparnis bietet das von der Stiftung Datenschutz angebotene digitale „Zentralarchiv für Tätigkeitsberichte der Bundes- und der Landesdatenschutzbeauftragten sowie der Aufsichtsbehörden für den Datenschutz", kurz ZAfTDa. Unter zaftda.de sind die seit 1971 veröffentlichten Tätigkeitsberichte der deutschen Aufsichtsbehörden für den Datenschutz abrufbar. Auch sind die Jahresberichte des Europäischen Datenschutzbeauftragten (aktuell 18), des Europäischen Datenschutzausschusses (4) und der Artikel 29-Gruppe (16 Berichte bis 2012) archiviert. Ferner sind Berichte der Datenschutzbeauftragten der Rundfunkanstalten sowie der katholischen und evangelischen Kirche archiviert. In der Rubrik „Neuer TB" wird auf neu erschienene Tätigkeitsberichte hingewiesen, sodass Interessierten eine zeitintensive Recherche in den vielen Internetangeboten der Datenschutzbehörden nach aktuellen Neuerscheinungen erspart bleibt.

Eine zusätzliche Recherchehilfe bietet die Stiftung Datenschutz mit einem speziellen E-Mail-Service an. Ist ein neuer Tätigkeitsbericht beim ZAfTDa abrufbar, werden die Nutzer:innen des Service via E-Mail benachrichtigt. Für die Anmeldung zu diesem Infoservice reicht eine formlose E-Mail an zaftda-news@stiftungdatenschutz.org aus.

Beschäftigtendatenschutz in der Praxis

Gemäß den Vorgaben des Betriebsverfassungsgesetzes und der Landespersonalvertretungsgesetze haben sich Betriebs- und Personalräte darum zu kümmern, dass die zugunsten der Arbeitnehmer geltenden Gesetze und Verordnungen durchgeführt werden. Dazu

zählt der Beschäftigtendatenschutz. Daraus ergibt sich die Verpflichtung für Betriebs- und Personalräte die Umsetzung des Datenschutzes bei der Betriebs- und Personalratsarbeit und im Betriebs- und Personalratsbüro sicherzustellen. In der Praxis sind diese gesetzlichen Aufträge nicht immer einfach umzusetzen. Die Tätigkeitsberichte können da eine Hilfe bieten, indem sie über eine Vielzahl von Fallgestaltungen zum Beschäftigtendatenschutz informieren.

Folgend einige Beispiele aus den Berichten zum Thema Beschäftigtendatenschutz.

Betriebliche WhatsApp-Nutzung – Finger weg!

Die Kommunikation mit dem WhatsApp-Messenger im privaten Bereich ist für viele so selbstverständlich, dass sie diesen Kommunikationskanal wie selbstverständlich auch in der betrieblichen Praxis verwenden. In den Tätigkeitsberichten werden immer neue Varianten der betrieblichen WhatsApp-Nutzung beschrieben und datenschutzrechtlich bewertet.

So berichtet die frühere **Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI)**, Maja Smoltczyk, in ihrem Bericht für das Jahr 2019 (Seite 123) über einen Berliner Arbeitgeber, der die fristlose Kündigung eines Arbeitsverhältnisses über einen WhatsApp-Gruppen-Chat des Unternehmens, der eigentlich zur Koordination genutzt wurde, allen Beschäftigten bekannt machte. Dazu versendete er eine Fotografie des Kündigungsschreibens, dem auch zu entnehmen war, dass dem Gekündigten ein Darlehen für den Ausgleich privater Zahlungsverpflichtungen vom Unternehmen gewährt worden war.

Der Berliner Datenschutzbeauftragten gefiel dieses Vorgehen nicht. Zwar erlaubt der § 26 BDSG die Verarbeitung von Beschäftigtendaten, wenn dies für Durchführung und Beendigung des Beschäftigungsverhältnisses erforderlich ist. Die Weiterleitung eines Kündigungsschreibens an eine firmeninterne WhatsApp-Gruppe könne aber kaum erforderlich sein und sei daher regelmäßig rechtswidrig. Die Einschätzung der Datenschutzbeauftragten geht weiter: „Im Übrigen ist der Einsatz von WhatsApp im Beschäftigungsverhältnis auch für Koordinierungszwecke im Unternehmen mit Vorgaben zum Beschäftigtendatenschutz, wie z.B. zur Speicherbegrenzung und zur Integrität und Vertraulichkeit kaum vereinbar und war hier unverzüglich abzustellen. (...) Der Einsatz von WhatsApp im Beschäftigungsverhältnis birgt erhebliche Risiken für das Persönlichkeitsrecht der Beschäftigten und ist daher regelmäßig unzulässig."

Über einen besonderen Fall berichtete die **Landesbeauftragte für Datenschutz und Informationsfreiheit in NRW** in ihrem Bericht für 2019 (Seite 51). Praktisch, dachte sich wohl ein Arbeitgeber, was man mit WhatsApp so alles machen kann. Er forderte die Beschäftigten seines Unternehmens schriftlich dazu auf Krankmeldungen nebst Belegen mit dem amerikanischen Instant-Messaging-Dienst an die Personalabteilung zu schicken. Nach einer Beschwerde prüfte die Datenschutzbehörde das Unternehmen und erhielt vom Arbeitgeber die Mitteilung, dass es sich dabei um ein zusätzliches Angebot an die Beschäftigten handle und überdies die Datenübermittlung wegen einer Ende-zu-Ende-Verschlüsselung sicher sei. Dem wollte sich die NRW-Datenschutzaufsicht nicht anschließen, weil mit der Nutzung von WhatsApp erhebliche Risiken durch die Möglichkeit des Datenzugriffs durch Unbefugte wie zum Beispiel durch Facebook verbunden sind. Facebook kann, und das gilt auch bei einer Ende-zu-Ende-Verschlüsselung, „auf die Verkehrsdaten (Wer kommuniziert wann mit wem?) und auf die Bestandsdaten (Wer ist für den Dienst angemeldet?) der Nachrichten zugreifen. Zudem liest die App das Adressbuch auf dem Gerät des Nutzers aus und gleicht die Daten mit den bei WhatsApp gespeicherten Daten ab, unabhängig davon, ob die Nutzer, auf die sich die Daten beziehen, davon wissen oder dies wollen."

Da der Arbeitgeber keinen Einfluss auf die Datenverarbeitungsvorgänge bei WhatsApp oder Facebook habe, stünden ihm die erforderlichen technisch-organisatorischen Mittel für einen effektiven Schutz der Beschäftigtendaten nicht zur Verfügung. Bei einer Nutzung von WhatsApp verstoße er daher auch gegen die Grundsätze der Datensicherheit, wie sie gemäß Art. 32 und 5 Abs. 1f der DSGVO umzusetzen sind. Ein weiteres Risiko bestehe auch darin, dass die Endgeräte sowohl des Arbeitsgebers als auch der Beschäftigten häufig nicht hinreichend abgesichert seien.

Versendung eines Sozialplans an Beschäftigte

Die Erstellung eines Sozialplans ist für Betriebsrat und Arbeitgeber keine leichte Sache, insbesondere, wenn er betriebsbedingte Kündigungen von Beschäftigten regelt. Aber auch bei dem Umgang mit einem Sozialplan ist der Datenschutz zu beachten. Über einen nicht datenschutzkonformen Umgang mit einem Sozialplan berichtet die **Bremer Landesbeauftragte für Datenschutz und Informationsfreiheit,** Dr. Imke Sommer, in ihrem Tätigkeitsbericht für das Jahr 2021 (Seite 52). Einem Hersteller von Computer-Hard- und -Software geriet der Datenschutz aus dem Blick; er verschickte im Rahmen einer betriebsbedingten Kündigung einen Sozialplan an die Beschäftigten, der unter anderem neben einer Namensliste Angaben zu Familienstand, Unterhaltspflichten, Geburtsdatum, Beschäftigungsdauer, Betriebsratszugehörigkeit und Schwerbehinderung der betroffenen Beschäftigten enthielt. Nach einem Hinweis der Datenschutzbehörde an das Unternehmen, dass ein solches Vorgehen datenschutzrechtlich unzulässig ist, wurde ein erneutes Anschreiben an die Beschäftigten verschickt. Diesem war die entsprechende Liste erneut beigefügt, die Namen waren jedoch geschwärzt worden. Das Unternehmen meinte, damit seien die Daten anonymisiert. Die Datenschutzbehörde sah darin aber lediglich eine Pseudonymisierung, da aufgrund der übrigen Daten weiterhin Rückschlüsse auf die betroffenen Personen möglich waren. Nach einem erneuten Hinweis der Aufsichtsbehörde auf die datenschutzrechtliche Unzulässigkeit auch dieser Versendung des Sozialplanes teilte das Unternehmen mit, „dass die Beschäftigten zur Vernichtung der fälschlicherweise erhaltenen Daten aufgefordert worden seien. Darüber hinaus seien Sensibilisierungsmaßnahmen durchgeführt und eine Anpassung der Arbeitsabläufe initiiert worden, um der-

artige Datenschutzverstöße zukünftig zu vermeiden".

Umgang mit Arbeitsunfähigkeitsbescheinigungen

Der Betriebsrat eines großen Unternehmens in Thüringen wandte sich mit der Frage an den **Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit,** Dr. Lutz Hasse, wie lange der Arbeitgeber die krankheitsbedingten Fehltage der Beschäftigten aufbewahren dürfe beziehungsweise ob eine konkrete Speicherdauer von fünf Jahren zu lang bemessen sei. Der Arbeitgeber wollte diese Daten offensichtlich nutzen, um einzelnen Beschäftigten das Arbeitsverhältnis aus krankheitsbedingten Gründen zu kündigen (3. TB DSGVO, Seite 152).

Da sich für privatwirtschaftliche Unternehmen, anders als in den Bundesländern für die Behörden, weder im Datenschutzgesetz noch im Entgeltfortzahlungsgesetz hierzu eine Regelung findet, verwies der Datenschutzbeauftragte zunächst auf den Grundsatz der Speicherbegrenzung nach Art. 5 Abs. 1 lit. e) DSGVO.

Nach dieser Regelung sind Beschäftigtendaten zu löschen, wenn der Zweck der Datenverarbeitung wegfällt. Das gilt nicht, wenn spezifische gesetzliche Aufbewahrungspflichten bestehen. Was aber bedeutet „erforderlich" hinsichtlich der Aufbewahrungs- und Speicherdauer von Arbeitsunfähigkeitsbescheinigungen und Zeiten der krankheitsbedingten Abwesenheit von Beschäftigten?

Bei einer krankheitsbedingten Kündigung ist der Arbeitgeber gegenüber den betroffenen Beschäftigten für das Vorliegen der Kündigungsgründe darlegungs- und beweispflichtig: „Das heißt, der Arbeitgeber muss darlegen und beweisen können, wie lange ein Arbeitnehmer innerhalb eines gewissen Zeitraumes vor Ausspruch der Kündigung krankheitsbedingt gefehlt hat und es müssen zum Zeitpunkt der Kündigung Tatsachen vorliegen, die eine Prognose weiterer Erkrankungen wie im bisherigen Umfang erwarten lassen (§ 1 Abs. 2 Satz 4 Kündigungsschutzgesetz)."

Auch wenn sich eine schematische Festlegung des Referenzzeitraumes für eine Negativprognose angesichts des breiten Spektrums möglicher Krankheitsbilder verbietet, kommt der Datenschützer bei seiner Abwägung zu dem Ergebnis, dass als Richtwert eine Zeit von mindestens zwei Jahren anerkannt werden müsse, um sicherzustellen, dass die Prognose ausreichend begründet werden kann. Unter Berufung auf die Rechtsprechung des Bundesarbeitsgerichts (Urteil vom 25. April 2018 – 2 AZR 6/18) hält der Datenschutzbeauftragte im Regelfall eine Speicherung der Krankheitszeiten von drei Jahren für ausreichend. Das BAG hat dazu ausgeführt: „Bei einer Kündigung wegen häufiger Kurzerkrankungen, vorbehaltlich besonderer Umstände des Einzelfalls, ist für die Erstellung der Gesundheitsprognose ein Referenzzeitraum von drei Jahren vor Zugang der Kündigung maßgeblich. Ist eine Arbeitnehmervertretung gebildet, ist auf die letzten drei Jahre vor Einleitung des Beteiligungsverfahrens abzustellen."

Eine darüberhinausgehende Speicherdauer von fünf Jahren hält der Thüringer Landesdatenschutzbeauftragte daher für zu lange. Eine Verlängerung der Dreijahresfrist sei nur möglich, wenn der Arbeitgeber dies im Einzelfall besonders begründet und diese Begründung hinreichend dokumentiert. Vorsorglich wird noch darauf hingewiesen, dass Beschäftigte nicht verpflichtet sind, die Diagnose ihrer Erkrankung dem Arbeitgeber mitzuteilen. Diese ergibt sich auch nicht aus der dem Arbeitgeber vorzulegenden AU-Bescheinigung über das Bestehen der Arbeitsunfähigkeit nach § 5 Entgeltfortzahlungsgesetz.

Datenpanne beim Personalrat

Betriebs- und Personalräte haben in ihrem Verantwortungsbereich die Datenschutzbestimmungen umzusetzen und sicherzustellen. Dazu gehört auch die Umsetzung technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Beschäftigtendaten. Was dabei zu beachten ist, musste sich ein Personalrat einer bayerischen Gemeinde vom **Bayerische Landesbeauftragten für den Datenschutz,** Prof. Dr. Thomas Petri, aus nicht gerade erfreulichem Anlass sagen lassen (30. TB, Seite 173).

Ein Personalratsmitglied hatte nach einer Personalratssitzung seinen Aktenordner, der die Unterlagen für die Personalratssitzung enthielt, auf dem Rückweg in sein Büro verloren. Auch nach intensiver Suche blieb der Ordner verschollen. Nach der Erinnerung des Personalratsmitglieds konnte der Inhalt des Aktenordners mit dem Ergebnis rekonstruiert werden, dass im Hinblick auf den Datenschutz insgesamt über 30 Personen vom Verlust der verlorenen Unterlagen betroffen waren. Eine Risikoeinschätzung der Unterlagen ergab, dass der Verlust der Unterlagen für über zehn betroffene Personen voraussichtlich ein hohes oder sehr hohes Risiko zur Folge haben könnte. Nachdem die Gemeinde die betroffenen Personen über den Verlust der Akte informiert hatte, reichte eine der betroffenen Personen eine Beschwerde bei der Datenschutzaufsichtsbehörde ein.

Neben einer datenschutzrechtlichen Beanstandung der Gemeinde hielt die Aufsichtsbehörde fest, dass der Personalrat auf die wirksame Umsetzung technischer und organisatorischer Schutzmaßnahmen achten muss. Dazu gibt sie folgende Hinweise:

Risikoanalyse durchführen: Das Risiko, sensible Personalratsunterlagen zu verlieren, ist eines von mehreren Risikoszenarien, das bei der entsprechend durchzuführenden datenschutzrechtlichen Risikoanalyse zu betrachten ist. In aller Regel sind nach der Bewertung des Ausgangsrisikos geeignete Schutzmaßnahmen wirksam umzusetzen, um dieses Risiko auf ein vertretbares Niveau zu reduzieren.

Transport vermeiden: Bestehende Potenziale, sensible Personalratsunterlagen nicht unnötig zu transportieren, sind zu realisieren. Dabei können digitale Hilfsmittel, beispielsweise eine zentrale digitale Ablage mit geeignetem Zugriffsschutz und weiteren Sicherheitsvorkehrungen, von Nutzen sein.

Transport absichern: Sensible Personalratsunterlagen, bei denen ein Transport unverzichtbar ist, müssen geeignet abgesichert transportiert werden. Je nach Risikolage ist etwa bei Papierunterlagen auf verschlossene Sicherheitstransportbehälter und bei Digitalunterlagen auf geeignete Verschlüsselung zu achten.

Konsequent löschen: Sobald Personalratsunterlagen für den ursprünglichen Verarbeitungszweck nicht mehr notwendig sind sind diese zu löschen oder zu anonymisieren.

GPS-Tracking im Beschäftigungsverhältnis

In zunehmendem Maße rüsten Unternehmen – vor allem in der Logistikbranche – ihre Fahrzeuge mit GPS aus. GPS steht für Global Positioning System (globales Positionsbestimmungssystem), offiziell NAVSTAR GPS. Die Technologie beruht auf einem Satellitensystem zur exakten Navigation oder Positionsbestimmung. Zur Nachverfolgung von Fahrzeugen werden diese mit einem GPS-Gerät ausgestattet.

Auf Grund einer Beschwerde gegen ein international tätiges Transportunternehmen überprüften der **Hessische Beauftragte für Datenschutz und Informationsfreiheit (HBDI)**, Prof. Dr. Alexander Roßnagel, und seine Mitarbeiter:innen im 50. Tätigkeitsbericht für 2021 (Seite 134) den Einsatz und die Anwendungen der eingesetzten Verfolgungstechnologie. Der Beschwerdeführer hatte vorgetragen, dass GPS-Tracker in die genutzten Fahrzeuge neu eingebaut worden seien und der Arbeitgeber den Einsatz gegenüber den Beschäftigten mit Diebstahlsicherung, Effizienzsteigerung, Verbesserung der Dienstleistung, Kontrolle unerlaubter Privatnutzung und Sicherheit der Fahrerinnen und Fahrer sowie der Fahrzeuge begründet hatte.

Folgende Daten würden sechs Monate gespeichert: Name des Fahrzeugbenutzers, der aktuelle Standort des Fahrzeuges, die aktuelle Geschwindigkeit des Fahrzeuges und die aktuellen Can-Bus-Daten (d.h. Zündung, Kilometerzähler, Kraftstoffverbrauch, Füllstand, Motorumdrehungen). Zu den Verarbeitungszwecken wurde von dem Transportunternehmen ausgeführt, dass das GPS-Tracking

- der schnellen Störungsbehebung und Effizienzsteigerung in der Routenplanung,
- der Sicherstellung der Einhaltung steuerrechtlicher Vorschriften,
- der Sicherheit der Fahrer (Unfall/Pannenhilfe),
- der Sicherheit der Fahrzeuge (Diebstahlschutz),
- der Effizienzsteigerung in der Fahrzeugbeschaffung (Qualität/Abnutzung der Fahrzeuge) und
- der Sicherstellung der Einhaltung arbeitsrechtlicher Vorgaben (Missbrauch der Tankkarte)

diene.

Das Prüfverfahren durch die Datenschutzaufsicht ergab, dass der Einsatz der GPS-Tracker in der vom Unternehmen beschriebenen Ausgestaltung gegen den Datenschutz verstieß. Prüfmaßstab war der § 26 Abs. 1 BDSG, der vorgibt, dass Beschäftigtendaten nur verarbeitet werden dürfen, wenn dies für die Durchführung des Beschäftigungsverhältnisses ‚erforderlich' ist. Dazu wird im Bericht ausgeführt: „Insbesondere wenn es um die Verarbeitung von Beschäftigtendaten geht, sind im Rahmen der Erforderlichkeitsprüfung die betroffenen Grundrechtspositionen und widerstreitenden Interessen zur Herstellung praktischer Konkordanz abzuwägen und zu einem Ausgleich zu bringen, der die Interessen der Beschäftigten und des Arbeitgebers möglichst weitgehend berücksichtigt (BT-Drs. 18/11325, 98). Gefordert wird hierfür eine Prüfung am Maßstab des Verhältnismäßigkeitsgrundsatzes, was wiederum voraussetzt, dass der Verantwortliche einen legitimen Zweck verfolgt, das Verarbeitungsverfahren für die Verwirklichung dieses Zwecks geeignet ist und es sich um das mildeste aller gleich effektiv zur Verfügung stehenden Mittel handelt (vgl. 9.04 2019 – 1 ABR 51/17) Darüber hinaus muss es auch unter Abwägung der Umstände des Einzelfalles angemessen sein."

Unter Anlegung dieses Maßstabes werden im Bericht die verschiedenen Tracking-Ziele geprüft:

- Schnelle Störungsbehebung und Effizienzsteigerung bei der Routenplanung

Hier kommt der Datenschützer zu dem Ergebnis, dass Störungsbehebung und Effizienzsteigerung bei der Routenplanung legitime Zwecke gem. § 26 Abs. 1 BDSG sind. Allerdings sei eine Speicherung der erhobenen GPS-Tracking-Daten hierfür nicht erforderlich und damit unzulässig, da zur Verwirklichung der genannten Zwecke eine „flüchtige Momentaufnahme", also lediglich die Verwendung aktuell zur Verfügung stehender Daten, ausreichend sei.

- Sicherheit der Fahrer (Unfall/Pannenhilfe)

Die Erhebung und Speicherung von GPS-Tracking-Daten, um bei einem Unfall oder einer Panne schnelle Hilfe zu leisten, könne als Maßnahme des Arbeitsschutzes gem. § 26 Abs. 1 Satz 1 BDSG in Verbindung mit den Bestimmungen des Arbeitsschutzgesetzes grundsätzlich als zulässig angesehen werden. Im konkreten Fall bezweifelt der Datenschutzbeauftragte die Geeignetheit der Maßnahme, da die im Falle eines Unfalls zur Verfügung stehenden Instrumente (Pannenhilfe, Notruf) für die Sicherheit der Fahrer geeigneter sein dürften. Eine dauerhafte Speicherung der GPS-Fahrzeug-Daten sei für die Zweckerfüllung nicht erforderlich.

- Sicherheit der Fahrzeuge (Diebstahlschutz)

Für den Diebstahlschutz und das Wiederauffinden eines Firmenfahrzeuges sei eine ständige Erfassung der Fahrzeugposition und eine Speicherung nicht erforderlich, da für das Wiederauffinden eines entwendeten Fahrzeuges die anlassbezogene Erhebung des Standorts des Fahrzeugs im Falle eines festgestellten Fahrzeugverlustes genügt.

- Effizienzsteigerung in der Beschaffung (Qualität, Abnutzung der Fahrzeuge)

Viele LKW-Daten und auch das Verhalten von Fahrer:innen können heute mittels einer Flotten-Management-Schnittstelle in Echtzeit-Überwachung durch die Firmenzentrale kontrolliert werden. Fahrzeugdaten wie etwa Zündung an/aus, Geschwindigkeit, Drehzahl, km-Stand, Tankinhalt, Kraftstoffverbrauch (Live Can Bus-Daten) werden automatisiert ausgelesen und übermittelt. Auch eine Fahrstilanalysen und die Protokollierung von Lenk- und Ruhezeiten ist möglich. Auf Grundlage der erhobenen

Daten kann, so der HBDI, ein Unternehmen auch die Leistung von Fahrzeugen beurteilen und entscheiden, ob der Fahrzeugtyp für den verwendeten Zweck geeignet ist oder ob zukünftig andere Fahrzeugtypen angeschafft werden, die z.B. einen geringeren Verbrauch aufweisen. Darüber hinaus könne auch relevant sein, ob Maximalkilometervorgaben eingehalten werden, die gemäß den jeweils anwendbaren Leasingverträgen berücksichtigt werden müssen.

- Sicherstellung der Einhaltung arbeitsrechtlicher Vorgaben

Zu unterscheiden sind anlasslose präventive Kontrollmaßnahmen zur Überprüfung der Einhaltung von bestehenden arbeitsrechtlichen Pflichten und anlassbezogene repressive Mitarbeiterkontrollen bei einem konkret zu dokumentierenden Anfangsverdacht.

Hinsichtlich anlassloser präventiver Kontrollmaßnahmen zur Überprüfung der Einhaltung von bestehenden arbeitsrechtlichen Pflichten hält der Datenschutzbeauftragte fest, dass präventive Compliance-Kontrollen, die nicht auf einem personenbezogenen einfachen Anfangsverdacht einer Pflichtverletzung oder einer Straftat bezüglich eines bestimmten Beschäftigten beruhen, unter bestimmten Voraussetzungen nach der Rechtsprechung des Bundesarbeitsgerichts auf § 26 Abs. 1 Satz 1 oder 2 BDSG gestützt werden können (BAG 09.07.2013 – 1 ABR 2/13, Rn. 20 ff.). Dies gelte vor allem für nach abstrakten Kriterien durchgeführte, keinen Arbeitnehmer besonders unter Verdacht stellende, offene, temporäre und stichprobenartige Überwachungsmaßnahmen, die der Verhinderung von Pflichtverletzungen oder Straftaten dienen sollen und ohne deren Durchführung keine verhaltenslenkende Wirkung entfaltet werden kann. Eine solche Maßnahme sei allerdings anzukündigen.

Eine anlassbezogene repressive Mitarbeiterkontrolle bei konkret zu dokumentierendem Anfangsverdacht einer Straftat müsse angesichts der konkret auf eine Person gerichteten Überwachung als erheblicher Eingriff in deren Persönlichkeitssphäre angesehen werden. Damit ein Ortungssystem zur Aufdeckung einer Straftat zulässig eingesetzt werden kann, sei es nach § 26 Abs. 1 Satz 2 BDSG notwendig, dass ein konkreter Anfangsverdacht einer Straftat vorliegt. Das besondere Zulässigkeitserfordernis eines konkreten Tatverdachts soll verhindern, dass eine gezielte Überwachung schrankenlos eingesetzt werden darf. Damit ein konkreter Tatverdacht vorliegt, so der Datenschutzbeauftragte, müssen Tatsachen gegeben sein, die als Indizien für das Vorliegen einer Straftat gelten können. Es müsse in persönlicher und räumlicher Hinsicht der objektiv begründete Anfangsverdacht einer Straftat bestehen.

Allerdings müsse bei einer repressiven Ortung mittels GPS-Tracker zwecks Aufklärung einer Straftat ein berechtigtes Interesse des Arbeitgebers an der Kontrollmaßnahme vorliegen und sein Interesse an der Aufdeckung der Straftat den schutzwürdigen Arbeitnehmerinteressen an der Wahrung seines Persönlichkeitsschutzes überwiegen, wobei bei der Interessenabwägung vor allem die Art und Schwere der Straftat, der Grad des Tatverdachts und die Schwere des Eingriffs in das Persönlichkeitsrecht zu berücksichtigen seien. So könnten sich etwa bei Bagatelldelikten Kontrollmaßnahmen verbieten. Grundsätzlich erlaubten präventive als auch repressive Maßnahmen keine dauerhafte und umfassende Ortung von Beschäftigten; die Überwachungsmaßnahme sei zeitlich zu begrenzen.

Angesichts der vielfältigen Überwachungsmöglichkeiten von Beschäftigten mittels GPS-Tracking empfiehlt der Hessische Datenschutzbeauftragte Betriebs- und Personalräten den Abschluss einer Betriebsvereinbarung vor der Einführung der Technologie.

Was darf in Dienstplänen mitgeteilt werden?

Online-Kalender und -Terminplaner sind sicher eine praktische Angelegenheit und Arbeitserleichterung. Haben aber mehrere Kolleginnen und Kollegen Einsicht in solche Kalender, sind datenschutzrechtliche Aspekte zu beachten. So erreichten den **Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit** im Jahr 2019 gleich mehrere Anfragen aus Unternehmen und Behörden zur Zulässigkeit von für alle Beschäftigte einsehbaren Kalendern, Zeitplänen und Tabellen, in denen auch vermerkt wird, welche Beschäftigten wegen einer Erkrankung (des Mitarbeiters selbst oder eines Kindes) nicht bei der Arbeit waren (siehe 2. TB nach DSGVO, Seite 92). Für derart konfigurierte Kalender, aus denen für andere Beschäftigte Informationen zu Fehltagen aufgrund von Erkrankung zu ersehen sind, gibt es keine spezifische Rechtsgrundlage.

Mit § 27 im neuen Thüringer Datenschutzgesetz (ThürDSG) wurde eine spezielle Vorschrift zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten aufgenommen. Die Vorschrift erklärt die dienstrechtlichen Vorschriften §§ 79 bis 87 Thüringer Beamtengesetz (ThürBG) für entsprechend anwendbar.

Aus diesen Paragrafen ergibt sich, so der Beauftragte, mangels Erforderlichkeit keine Zulässigkeit die Gründe für private oder persönliche Abwesenheiten wie zum Beispiel Krankheit, Krankenhaus- oder Kuraufenthalt, Kinderbetreuung, Urlaub etc. anderen Beschäftigten via Terminkalender zur Kenntnis zu geben. Fazit des Datenschützers: „Anderen Beschäftigten darf allenfalls, sofern eine Erforderlichkeit begründet werden kann, zur Kenntnis gegeben werden, ob ein Mitarbeiter ansprechbar ist oder sich nicht im Dienst befindet. Hierzu reicht es aus, die betreffenden Mitarbeiter als ‚abwesend' zu kennzeichnen. Die Gründe der Abwesenheit sind nicht relevant und daher auch nicht zur Einsicht bereitzustellen. Lediglich im Falle einer dienstlich bedingten Abwesenheit, zum Beispiel wegen Dienstreise, bestehen keine Bedenken gegen eine Kenntnisnahmemöglichkeit, da es sich um ein dienstliches Datum handelt."

Soweit das Ergebnis für die Behörden in Thüringen. Die Regelungen in den anderen Landesdatenschutzgesetzen führen zu keinem anderen Ergebnis für die jeweiligen Landesbehörden. Und auch der § 26 BDSG (Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses) kommt für private Unternehmen zum gleichen Ergebnis.

Immer horche, immer gugge...

... sagt man in Hessen. Gut informierte Betriebs- und Personalräte sind eine Voraussetzung für eine gute Umsetzung von Beschäftigteninteressen. Das gilt auch für die aktuellen Entwicklungen beim Beschäftigtendatenschutz. Da ist es durchaus hilfreich, einmal in die Tätigkeitsberichte der Datenschutzbehörden zu „gugge".

* Der Autor berät und schult Betriebs- und Personalräte zum Beschäftigtendatenschutz. In der Zeitschrift Computer und Arbeit, Bund Verlag, berichtet er regelmäßig über Fälle zum Beschäftigtendatenschutz aus aktuell erschienen Tätigkeitsberichten der Datenschutzbehörden.

Dr. Frank Schury, Riko Pieper

Ein Weg zur Umsetzung des neuen § 79a BetrVG „Datenschutz" in der Praxis – Oder: „Geltendes Recht ist anzuwenden ?!?"

Vorbemerkung

Die vorrangige Zielsetzung des nachfolgenden Beitrags ist nicht eine umfassende Behandlung bzw. endgültige juristische Beurteilung aller Argumente hinsichtlich der DSGVO-Konformität des § 79a[1] BetrVG. Es geht den Autoren vielmehr darum zu zeigen, welchen Weg der Konzerndatenschutz der DFS gewählt hat die Bestimmungen dieses Paragrafen umzusetzen.

Rahmenbedingungen der DFS Deutsche Flugsicherung GmbH

Die DFS Deutsche Flugsicherung firmiert als GmbH in Konzernstruktur mit zum Teil internationalen Töchtern und Niederlassungen in allen Bundesländern. Sie nimmt im Auftrag des Bundes die hoheitliche Aufgabe Flugverkehrskontrolle wahr. Somit gilt sie, trotz der Rechtsform GmbH, gemäß § 2[2] Abs. 4 Satz 2 BDSG als „öffentliche Stelle im Sinne dieses Gesetzes". Die zuständige Datenschutz-Aufsichtsbehörde der DFS für das Kerngeschäft ist daher der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit BfDI[3]. Die DFS als Rechtsnachfolger der ehemaligen Bundesbehörde Bundesanstalt für Flugsicherung (BFS) hat unter den Beschäftigten zugewiesene Beschäftigte des Luftfahrtbundesamts und aufgrund der zivil-militärischen Zusammenarbeit auch beurlaubte Soldaten.

Die DFS finanziert sich im Kerngeschäft über Flugsicherungsgebühren, die Luftraumnutzer für An-/Abflug und Strecke bezahlen. Der Anteilseigner Bund hat zusätzlich in der DFS-Strategie den Ausbau des preisfinanzierten Geschäfts verankert. Für dieses sogenannte „Drittgeschäft" wurden verschiedene Tochtergesellschaften gegründet oder aufgekauft, die größtenteils keinen hoheitlichen Auftrag haben. Die Tochtergesellschaften ohne hoheitlichen Auftrag haben ihren Sitz in Hessen und Bayern und sind somit „nicht-öffentliche Stellen" im Sinne des BDSG und der DSGVO. Zuständige Aufsichtsbehörden sind in diesen Fällen die jeweiligen Landesbehörden für den Datenschutz, der HBDI[4] und das BayLDA[5].

Vorgeschichte zum neuen § 79a BetrVG

Seit vielen Jahren gab es eine Rechtsunsicherheit bezüglich der Frage, ob der Betriebsrat (BR) Teil der „verantwortlichen Stelle" gemäß § 3[6] Abs. 7 BDSG a.F. bzw. seit 2018 „Verantwortlicher" gemäß Art. 4[7] Nr. 7 DSGVO ist. Sowohl für die Ablehnung als auch für die Unterstützung der Ansicht, den BR als Teil der verantwortlichen Stelle zu sehen, wurden Argumente vorgetragen:

- Ablehnende Haltungen referenzierten im Kern auf ein BAG-Urteil von 1997[8] und weitere Urteile, u. a. ein BAG-Urteil aus 2012[9] zur Internetnutzung durch BR-Mitglieder. In diesen Urteilen wird immer im Wesentlichen auf die Unabhängigkeit des BR abgestellt, was jegliche Kontrollrechte, sei es durch den Datenschutzbeauftragten (DSB) oder andere Stellen des Unternehmens, wie z. B. Administratoren, ausschließt. Dies wurde u. a. mit der Tatsache begründet, dass der DSB vom Arbeitgeber bestellt wird, und somit als „Erfüllungsgehilfe" oder gar als „Handlanger" des Unternehmens zu sehen wäre. Die Vertreter dieser Ansicht argumentierten mit dem direkten Weisungsrecht des Arbeitgebers gegenüber dem DSB, abgeleitet aus dem § 4f[10] (3) BDSG a.F., der von einer Unterstellung des DSB unter die oberste Leitung sprach.
Die Schweigepflicht des DSB, auch gegenüber dem Verantwortlichen, wurde nicht als hinreichendes Gegenargument akzeptiert, da sich diese Pflicht nur auf die personenbezogenen Daten bezieht, nicht aber auf weitergehende Informationen, wie z. B. Entscheidungsprozesse oder Beschlussfassungen des BR. Einzelne Vertreter forderten deshalb konsequent eine eigene Datenschutzorganisation des BR, inklusive der Bestellung eines eigenen DSB des BR, einzurichten (siehe Wedde 2020[11]).
- Die gegenläufige Ansicht, den BR als Teil der verantwortlichen Stelle zu sehen, basierte im Wesentlichen auf zwei Argumentationslinien:

In der Praxis nutzen Betriebsräte die Infrastruktur, die das Unternehmen zur Verfügung stellt und betreibt, und somit für die IT-Systeme auch die wesentlichen Pflichten hinsichtlich technischer und organisatorischer Maßnahmen (TOM) wahrnimmt. Dies manifestiert die Stellung des Arbeitgebers als Verantwortlicher für die Verarbeitung von personenbezogenen Daten.

Im Hinblick auf die o. g. Argumente, mit denen dem DSB Kontrollrechte abgesprochen wurden, hielt man nach Inkrafttreten der DSGVO und des BDSG in neuer Fassung entgegen, dass vom BAG 1997 ein Beschluss in einer Zeit gefasst wurde, in der man den DSB durchaus als „verlängerten Arm oder Handlanger des Arbeitgebers“ sehen konnte. Diese Meinung würde jedoch nicht mehr der aktuellen Rolle des DSB gerecht. Somit könne man sich auch nicht mehr auf dieses Urteil berufen. Damit würde ein wesentliches Argument, das gegen den Arbeitgeber als verantwortliche Stelle spricht, wegfallen.

Das Betriebsrätemodernisierungsgesetz – § 79a BetrVG „Datenschutz“ als Lösung?

Als Ergebnis der oben dargestellten Rechtsunsicherheit wurde der Gesetzgeber mehrfach aufgefordert für Klarheit zu sorgen. Im Jahr 2020 fasste die Datenschutzkonferenz einen Beschluss[12] an den Bundesgesetzgeber heranzutreten und diesen aufzufordern in Wahrnehmung seiner Spezifizierungsbefugnis nach Art. 4 Nr. 7 Hs. 2 i. V. m. Art. 88[13] Abs. 1 DSGVO gesetzlich klarzustellen, ob der BR Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO ist.

Der gemäß „Betriebsrätemodernisierungsgesetz“[14] im Jahr 2021 neu eingeführte § 79a BetrVG sollte die geforderte Rechtssicherheit schaffen, ob der BR als Verantwortlicher oder als Teil des Verantwortlichen im Unternehmen in Ausübung seiner Aufgaben personenbezogene Daten verarbeitet. Damit einhergehend entstünde dann auch Klarheit hinsichtlich der daraus erwachsenden Konsequenzen, speziell hinsichtlich der Kontrollrechte des DSB, der Verantwortlichkeit für TOM, der Umsetzung der Rechte der Betroffenen und Haftungsfragen bei Datenschutzverstößen.

Wie wurde die geforderte Rechtssicherheit nun durch den § 79a BetrVG umgesetzt:

„Bei der Verarbeitung personenbezogener Daten hat der Betriebsrat die Vorschriften über den Datenschutz einzuhalten. Soweit der Betriebsrat zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben personenbezogene Daten verarbeitet, ist der Arbeitgeber der für die Verarbeitung Verantwortliche im Sinne der datenschutzrechtlichen Vorschriften. Arbeitgeber und Betriebsrat unterstützen sich gegenseitig bei der Einhaltung der datenschutzrechtlichen Vorschriften. Die oder der Datenschutzbeauftragte ist gegenüber dem Arbeitgeber zur Verschwiegenheit verpflichtet über Informationen, die Rückschlüsse auf den Meinungsbildungsprozess des Betriebsrats zulassen. § 6 Absatz 5 Satz 2, § 38 Absatz 2 des Bundesdatenschutzgesetzes gelten auch im Hinblick auf das Verhältnis der oder des Datenschutzbeauftragten zum Arbeitgeber.“

Was wurde damit nun geschaffen? Die Verantwortlichkeit ist dem Arbeitgeber zugeordnet, die Verschwiegenheitspflicht des DSB wurde erweitert und die Zusammenarbeit zwischen Arbeitgeber und BR bei der Einhaltung der Bestimmungen ohne weitere Spezifizierung wurde manifestiert.

Klärungsprozess zur praktischen Umsetzung des § 79a BetrVG im DFS-Konzern

Die Klarheit bezüglich der Verantwortung des BR scheint auf den ersten Blick erfüllt zu sein. Der Arbeitgeber ist der Verantwortliche – mit allen sich daraus ergebenden Konsequenzen!

Bei näherer Betrachtung ist es aber so, dass die Schaffung einer Rechtssicherheit, trotz des klar zu erkennenden Willens des Gesetzgebers, nach wie vor strittig erscheint. Nachfolgend aufgeführte Punkte werden von Vertretern dieser Ansicht angeführt:

- Nach Art. 4 Nr. 7 Hs. 1 DSGVO ist Verantwortlicher, wer über die **Zwecke und Mittel** (Hervorhebung durch die Autoren) der Datenverarbeitung entscheidet. Das BetrVG regelt unstrittig an mehreren Stellen die Zwecke (Aufgaben) des BR. An keiner Stelle dieses Gesetzes sind aber die Mittel festgeschrieben. Über die Mittel zur Verarbeitung personenbezogener Daten durch den BR entscheidet der BR autonom. In diesem Punkt wurde das BetrVG nicht geändert.
- § 79a S. 2 BetrVG [...] ist weder von der Öffnungsklausel des Art. 4 Nr. 7 Hs. 2 DSGVO gedeckt noch ist er eine spezifischere Vorschrift zur Verarbeitung von Beschäftigtendaten im Beschäftigungskontext im Sinne des Art. 88 DSGVO. Wegen der unmittelbaren Geltung der DSGVO in allen Mitgliedstaaten der EU darf die Vorschrift deshalb nicht angewendet werden. Für die Datenverarbeitung durch den BR gilt daher Art. 4 Nr. 7 Hs. 1 DSGVO.
- Der Arbeitgeber haftet für Datenschutzverstöße seiner Betriebsräte grundsätzlich nicht.

Die aufgeführten Punkte sollen an dieser Stelle nicht im Einzelnen diskutiert werden. Den Autoren erschien aber insbesondere die Argumentation hinsichtlich der nichterfolgten Festlegung der Mittel im BetrVG durchaus nachvollziehbar.

Vor dem Hintergrund der Forderung der Datenschutzkonferenz Klarheit zu schaffen (s. o.), war es naheliegend die Sichtweisen der für den DFS-Konzern zuständigen Datenschutz-Aufsichtsbehörden BfDI, HBDI und BayLDA einzuholen. Alle drei Behörden wurden mit dem Hinweis auf die aktuell unterschiedlichen Rechtsauffassungen zu dem neuen § 79a BetrVG per E-Mail angeschrieben.

In dieser Mail wurden die oben aufgeführten Punkte dargestellt und zusätzlich auf praktische Probleme der Umsetzung hingewiesen, u. a. in Bezug auf Auskünfte gem. Art. 13[15] DSGVO in vertraulichen Vorgängen des BR durch den Arbeitgeber und die Frage nach der verantwortlichen Stelle bei Konzernbetriebsräten.

Alle drei Behörden beantworteten die Anfrage und boten einen weiteren Austausch zu dem Thema an. In diesem Dialog wurde in erster Linie erörtert, inwieweit der in Rede stehende § 79a BetrVG eine Öffnungsklausel im Sinne des Art. 4 Nr. 7 Hs. 2 DSGVO darstellt

und wie die von den Autoren dargestellten Praxisprobleme zu lösen wären. Der Austausch mit den Datenschutz-Aufsichtsbehörden war dabei sehr konstruktiv und wurde von allen Beteiligten mit großer Offenheit und auch Interesse an den Positionen der jeweils anderen Behörden geführt.

Im Ergebnis war folgendes festzuhalten:

- § 79a BetrVG ist geltendes Recht und damit anzuwenden.
- Diese Regelung stellt eine Öffnungsklausel im Sinne des Art. 4 Nr. 7 Hs. 2 DSGVO dar. Für diese Rechtsauffassung wurden verschiedene Argumente aufgeführt:
  - Der BR sei analog dem DSB zu betrachten, der auch Teil der verantwortlichen Stelle sei. Ohne an dieser Stelle vertieft eine Diskussion über die Rechtsstellung des DSB zu beginnen, könnte man auch zum Umkehrschluss kommen: Der DSB, da er ebenfalls ohne gesetzliche Vorgabe zur Wahl der Mittel seine Aufgaben nach DSGVO erfüllt, müsste auch verantwortliche Stelle sein. Das hätte etwas von der Büchse der Pandora.
  - Es wurde die Regelung der Auftragsverarbeitung angeführt, bei der das Unternehmen verantwortliche Stelle bleibt, obwohl der Auftragnehmer bei der Wahl nicht wesentlicher Mittel der Verarbeitung wie Hard- und Software frei entscheiden kann. Diese Sichtweise wird durch ein Leitlinienpapier des Europäischen Datenschutzausschusses zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO[16] unterstützt. Dementsprechend könne man eine Analogie zum Verhältnis BR zum Arbeitgeber sehen.
- Die von den Autoren aufgeführten Bedenken, insbesondere hinsichtlich verschiedener Umsetzungsprobleme in der Praxis, könne man aber trotzdem durchaus nachvollziehen. Die Autoren wurden an dieser Stelle auch auf entsprechende Bedenken des LfDI Baden-Württemberg Dr. Brink[17] verwiesen, der im Ergebnis zwar auch feststellt, dass § 79a BetrVG geltendes Recht und damit anzuwenden sei, aber auf Grund durchaus diskussionswürdiger Einwände in einem Fachaufsatz die nachfolgende Befürchtung äußert:
  „…So ist zu befürchten, dass sich um die Durchsetzung von § 79 a BetrVG nF zunächst die Arbeitsgerichte werden bemühen müssen."

„Alles klar - was nun?" – Weiteres Vorgehen im DFS-Konzern

Das Ergebnis war somit erst einmal eindeutig: § 79a BetrVG ist anzuwenden, auch wenn einzelne Bedenken der Autoren nicht vollkommen ausgeräumt wurden. So ist im Hinblick auf die beschriebenen Analogien zum DSB bzw. der Auftragsverarbeitung zumindest einzuwenden, dass in beiden Fällen, anders als beim BR, weitere Regelungen existieren, die das Verhältnis zum Unternehmen bestimmen. Beim DSB ist dies die Benennung durch den Arbeitgeber und beim Auftragnehmer die Vereinbarung zur Auftragsverarbeitung mit dem Unternehmen. Eine „1:1"- Analogie zur Aufgabenerfüllung des BR liegt somit nicht vor.

Aus den eingangs beschriebenen Rahmenbedingungen resultieren im DFS-Konzern mehrere unterschiedliche Arbeitnehmervertretungen: Es gibt einen Konzernbetriebsrat (KBR), einen Gesamtbetriebsrat (GBR), achtzehn örtliche Betriebsräte an den Niederlassungen und einen Personalrat (PR).

Entsprechend der eingangs in der Vorbemerkung genannten Zielsetzung unseres Beitrags eine Lösung für die Umsetzung in der Praxis zu finden, wurde nun im nächsten Schritt auf die Arbeitnehmervertretungen und den zuständigen Personalbereich zugegangen. Die ersten Ergebnisse sehen wie folgt aus:

- Das Meinungsbild ist innerhalb der Arbeitnehmervertretungen uneinheitlich. Verschiedene Betriebsräte lehnen, basierend auf Aussagen von Referenten bei Datenschutzschulungen für Betriebsräte, die Regelungen des § 79a BetrVG ab.
- Betriebsräte der DFS arbeiten überwiegend im Netzwerk der DFS, die somit als Unternehmen die Einhaltung der Bestimmungen zu TOM gem. den Artt. 24 und 32 DSGVO sicherstellen muss.
- Sowohl auf Arbeitgeberseite als auch bei den Betriebsräten gibt es viele Fragen zur Umsetzung. Es wurde schon eine erste Liste mit Punkten erstellt, die in der praktischen Umsetzung schwierig bzw. strittig werden:
  - Integration des Verzeichnisses der Verarbeitungstätigkeiten (VVT) des BR in das VVT des Unternehmens.
  - Verantwortung bei Datenschutzverstößen, insbesondere bei Nichteinhaltung der Anforderungen an TOM.
  - Erfüllung der Anforderungen aus Kapitel 3[18] DSGVO „Rechte der Betroffenen".
  - Verantwortung für die Verarbeitung durch Betriebsräte des KBR, die jeweils verschiedenen Tochterunternehmen angehören.
  - Wahrnehmung der Kontrollrechte des DSB bei den Betriebsräten.

Bestreben der Autoren wird es sein zu den o. a. Punkten gemeinsame Regelungen im Sinne der in § 79a BetrVG geforderten gegenseitigen Unterstützung bei der Einhaltung der datenschutzrechtlichen Vorschriften zu finden. Mögliches Mittel wäre der Abschluss von Betriebsvereinbarungen, wie es der LfDI Baden-Württemberg Dr. Brink empfiehlt. Ziel muss es sein mittels eines „common sense" einen Weg zu bestreiten, der eine mögliche Flut von Gerichtsverfahren vermeidet.

1 http://www.gesetze-im-internet.de/betrvg/__79a.html

2 https://dsgvo-gesetz.de/bdsg/2-bdsg/

3 https://www.bfdi.bund.de/DE/Home/home_node.html

4 https://datenschutz.hessen.de/

5 https://www.lda.bayern.de/de/index.html

6 http://www.buzer.de/gesetz/3669/a51560.htm

7 https://dsgvo-gesetz.de/art-4-dsgvo/

8 http://archiv.jura.uni-saarland.de/jurpc/rechtspr/19980039.htm

9 https://www.mahnerfolg.de/urteile/index.php/internetzugang-betriebsrats-ueber-gruppenaccount/

10 http://www.buzer.de/gesetz/3669/a51568.htm

11 https://www.bund-verlag.de/aktuelles~Keine-Kontrolle-durch-Datenschutzbeauftragten-~.html sowie

Däubler/Wedde/Weichert/Sommer: EU-DSGVO und BDSG – Kompaktkommentar, 2. Auflage 2020, § 26 BDSG RN 269ff – ab Seite 1163

12 https://www.datenschutzkonferenz-online.de/media/pr/20200617_protokoll_99_dsk.pdf – TOP 15 Verantwortlichkeit des Betriebsrates

13 https://dsgvo-gesetz.de/art-88-dsgvo/

14 https://www.bgbl.de/xaver/bgbl/start.xav?start=//*%5B@attr_id=%27bgbl121s1762.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1762.pdf%27%5D__1663922078236

15 https://dsgvo-gesetz.de/art-13-dsgvo/

16 https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_de.pdf

17 http://beck-online.beck.de/Bcid/Y-300-Z-NZA-B-2021-S-1440-N-1

18 https://dsgvo-gesetz.de/kapitel-3/

Reinhard Linz

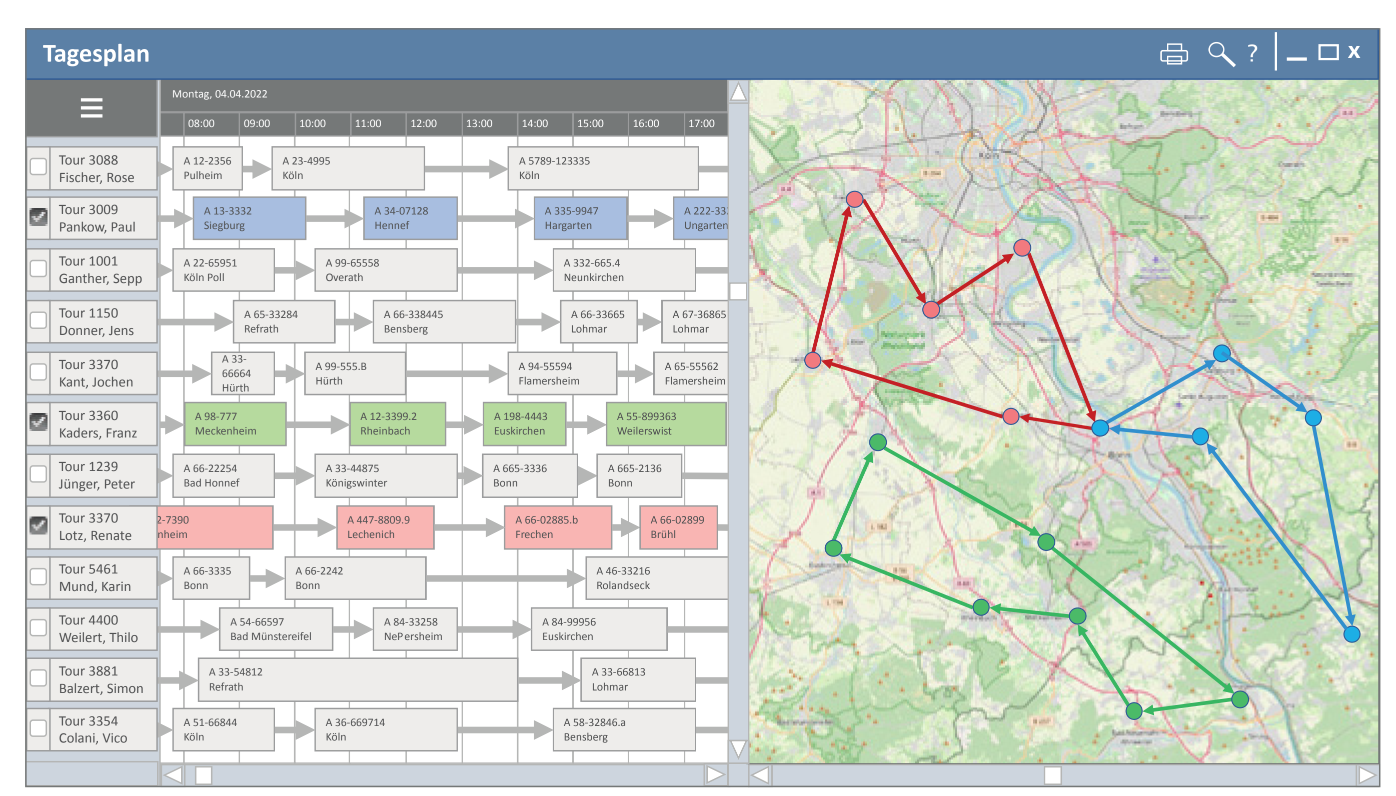
Personenbezogene Daten ohne Bedeutung?

Gibt es so etwas überhaupt – Daten ohne Bedeutung? Wenn ja, wer will solche Daten haben? Kann man damit irgendetwas Sinnvolles anfangen? Am Beispiel eines realen, hier modifiziert dargestellten Falls wollen wir diese vielleicht etwas skurrile Frage genauer unter die Lupe nehmen. Zum Ergebnis so viel vorweg: Die Bedeutung von Daten liegt manchmal versteckt jenseits ihres unmittelbaren Informationsgehalts.

Der Fall: Einfachere Tourenplanung durch IT-Unterstützung

Die ABC AG führt als Dienstleistung Reparaturen an technischen Anlagen aus, die bei ihren Kunden installiert sind. Dafür beschäftigt die ABC AG zahlreiche Techniker im Außendienst, die mit irgendwelchen Fahrzeugen zu den Kunden reisen, um dort die nötigen Arbeiten auszuführen. Die Techniker starten von verschiedenen Standorten des Unternehmens oder von ihren Wohnungen. Die Reparaturaufträge sind recht unterschiedlich. Manche Aufträge sind termingebunden, die Bearbeitungszeiten variieren zwischen einer Stunde und mehreren Tagen, und die benötigten Werkzeuge und Gerätschaften können manchmal nur in größeren Werkstattwagen oder gar LKW transportiert werden.

Für die Arbeitsplanung, also für die Frage, welche Techniker an welchen Tagen welche Aufträge bearbeiten sollen, ergibt sich ein komplexes Optimierungsproblem. Die Reisezeiten sollen möglichst kurz sein, um die teuren Arbeitskräfte möglichst produktiv einzusetzen, die Fahrstrecken sollen kurz sein, um die Fahrtkosten zu minimieren, Übernachtungen sollen vermieden werden, um Hotelkosten zu sparen, die Aufträge samt Fahrzeit sollen jeden Techniker an jedem Tag möglichst so lange beschäftigen, wie es seiner normalen Soll-Arbeitszeit entspricht, und alle Aufträge sind pünktlich zu erledigen.[1]



Hier verspricht ein Computersystem Hilfe. Es berechnet – so die Verheißung – den optimalen Tourenplan gewissermaßen auf Knopfdruck. Natürlich muss man das System mit den relevanten Merkmalen der Aufträge (Orte, Termine, Zeitbedarf usw.) füttern und auch mit einigen Charakteristika der verschiedenen Techniker: Wer kann welche Reparaturen ausführen? Wer startet wo? Wer hat welche Art von Fahrzeug? Und noch manches mehr. Das bei der ABC AG eingesetzte System erwartet, dass zu jedem Außendienst-Techniker neben vielen anderen die folgenden Angaben gespeichert werden:



Die „Objekte" sind hier die Außendienstmitarbeiter, der Personenbezug steht außer Frage.

Bessere Tourenplanung durch falsche Daten

Bei allen Bemühungen um die Bestimmung „korrekter" Parameter pro Techniker erwies sich das System bei der ABC AG leider doch nicht als der perfekte Tourenplaner. Zahlreiche Techniker beschwerten sich über zu viele Aufträge pro Tag, fehlende Gelegenheiten für Pausen, manchmal auch über nutzlose Wartezeiten zwischen Aufträgen, ungeschickte Fahrrouten und manches andere. Auch die Disponenten fanden mit Papier und Bleistift in etlichen Fällen Tourenpläne, die in ihren Augen besser passten als sie der Planungsalgorithmus konfiguriert hatte. Der Mangel wurde nicht als so gravierend eingestuft, dass man das ganze Programm abgeschafft hätte. Vielmehr versuchten die Disponenten die Tourenplanung dadurch zu verbessern, dass sie bei den unzufriedenen Technikern die oben genannten Parameter veränderten – was nach einigem Probieren tatsächlich gelang. Nun aber waren die Angaben nicht mehr zutreffend.

Dem Betriebsrat erschien es wichtiger, dass zufriedenstellende Tourenpläne entworfen würden als dass alle im System über die Außendienstler gespeicherten Angaben der Wahrheit entsprächen. In der einschlägigen Betriebsvereinbarung wurden diese Parameter deshalb ausdrücklich als „virtuell" eingestuft. Sie dürfen beliebig justiert werden.

Hier wird es interessant. Die Parameter sind zweifellos personenbezogene Daten. Schließlich stehen sie im Stammdatensatz jedes Außendienst-Technikers und können von Person zu Person variieren. Aber was sagen sie noch aus? Nachdem die Disponenten an den Werten „gedreht" haben, bis das System gute Touren lieferte, kann man sich auf die Richtigkeit der Angaben nicht mehr verlassen. Es ist nicht mehr sicher, dass in den Datenfeldern „drin ist, was draufsteht", und das hat hier sogar Methode. Was wird nun aus dem Auskunfts- und Korrekturanspruch, den das Gesetz, die DSGVO, den Betroffenen eigentlich garantiert? Kann ich eine Korrektur meiner Daten verlangen, wenn doch vereinbart ist, dass die Daten gar nicht korrekt zu sein brauchen, dass ihnen auch niemand die Bedeutung beimisst, die die Bezeichnungen der Parameter suggerieren, und dass die Daten auch nicht in diesem Sinne ausgewertet werden? Nach welchen Maßstäben soll ein Betroffener, wie es in der Betriebsvereinbarung bei der ABC AG vorgesehen ist, sein OK zu der Wahl der Parameter geben? Kann es den Betroffenen egal sein, welche Werte da gespeichert sind? Ist das Auskunfts- und Korrekturrecht also mangels Bedeutung der Daten sinnlos? Sicher nicht.

Bei den Parametern Fahrgeschwindigkeit und Arbeitsgeschwindigkeit ist es ganz offensichtlich, dass sie nur schwer objektiv zu bestimmen sind, und bei genauerem Hinsehen erweisen sich auch die anderen Parameter als diskussionsbedürftig. Deshalb wurde in einer Betriebsvereinbarung zu dem System festgelegt, dass die Techniker an der Festlegung der Parameter zu beteiligen sind.

Grundsätzlich aber handelt es sich bei diesen Angaben ganz klassisch um Daten, denen man eine bestimmte Bedeutung zumessen kann, bei Bedarf nach einer besonderen Klärung oder Übereinkunft. Im technischen Sinn sind das Datenfelder, die jeweils einen Aspekt des abgebildeten Objekts repräsentieren und deren Wertausprägungen das Objekt unter diesem Aspekt beschreiben. Die Bezeichnungen der Datenfelder geben einen Hinweis auf ihre Bedeutung.

Bedeutungslose, dennoch relevante Daten

Denn *praktisch* sind diese Parameter sehr wohl von Bedeutung. Schließlich beeinflussen sie die Einsatzplanung für jeden einzelnen Techniker in erheblichem Maße, führen zu kurzen oder weiten Fahrstrecken, mehr oder weniger Aufträgen pro Tag und bei einer wirtschaftlichen Erfolgsbeteiligung möglicherweise sogar zu höherem oder geringerem Einkommen. Die Bedeutung der Parameter liegt in der Art und Weise, in der sie verarbeitet werden, hier: Wie sie die Tourenplanung beeinflussen. Im Sinne der Semiotik könnte man sagen, die Bedeutung dieser Daten liegt nicht auf der semantischen, sondern auf der pragmatischen Ebene. Hier und nur hier spielt sich in diesem Fall das Entscheidende ab. Deshalb ist Transparenz für die

Betroffenen erst dann gegeben, wenn sie Kenntnis nicht nur über die zu ihrer Person gespeicherten Daten, sondern auch über die Art ihrer Verwendung haben.

Dies gilt keineswegs nur für das hier wiedergegebene Beispiel der ABC AG. Das Beispiel ist nur deswegen speziell (und damit besonders instruktiv), weil die individuellen Parameter für sich genommen überhaupt keine Bedeutung mehr haben. Aber selbst dann, wenn die Disponenten der ABC AG stets „wahre" Daten über die Außendienst-Techniker in den Planungsalgorithmus eingäben, bliebe ja der pragmatische Teil das eigentlich Interessante, das man nicht einfach ausblenden kann.

Ähnlich liegt der Fall auch bei den viel diskutierten Bonitätskennzahlen, die Banken von Kreditauskunfteien berechnen lassen und dann zur Grundlage von Kreditangeboten an ihre Kunden machen. Auch hier ist es für die Betroffenen nicht so wichtig, ob die Eingabewerte wie Alter, Geschlecht, Anstellungsverhältnis, Wohnanschrift etc. wahrheitsgemäß notiert sind; entscheidend ist das Kreditangebot, seine Konditionen und ggf. eine Begründung für die Kreditverweigerung, und das resultiert aus den Berechnungen des Bonitätsalgorithmus. Vergleichbar sind auch Systeme, die die Wortwahl und die Formulierungen in Bewerbungsschreiben analysieren, in Interviews vielleicht sogar die Sprachmelodie oder die Körperhaltung der Kandidaten untersuchen und zumindest eine Auswahlempfehlung für die Personalabteilung treffen. Weniger schwerwiegend, aber ebenfalls prägnant für unsere These sind die Algorithmen, die Tracking-Daten der Internet-Benutzer für die Auswahl von Werbeeinblendungen auf Webseiten verwenden. Hier gibt es überhaupt kein Berechnungsergebnis in Form eines Datums, über dessen Wert man Auskunft erteilen könnte. Das System reagiert einfach auf die Tracking-Daten durch eine bestimmte Werbeeinblendung. Sonst nichts.

Transparenz: Klarheit über Daten und ihre Nutzung

Damit Betroffene ihr Grundrecht auf informationelle Selbstbestimmung sinnvoll wahrnehmen können, müssen sie alles wissen, was für die Beurteilung der sie betreffenden Datenverarbeitung wichtig ist. Wenn nun die Bedeutung eines Datums auch oder allein darin besteht, wie es sich auf einen bestimmten Algorithmus – etwa zum Entwurf eines Tourenplans – auswirkt, kann man die Relevanz, die Kritikalität und auch die Richtigkeit des Datums nur im Hinblick auf diesen Verwendungskontext beurteilen. Ein Datum wäre dann für einen Betroffenen relevant und vielleicht besonders kritisch, wenn es als Eingabeparameter den Algorithmus und das Berechnungsergebnis stark beeinflusst. Und wann könnte man einen für sich genommen bedeutungslosen Parameter etwa des Tourenplanungsalgorithmus „richtig" nennen? Die naheliegende Antwort lautet: Dann, wenn der Parameter zu einem tatsächlich optimalen Ergebnis führt.

Hier wird die Sache reichlich komplex und damit zum Problem. So ist die Wirkung einzelner Parameter auf das Berechnungsergebnis des Algorithmus, z.B. auf den Tourenplan, vermutlich gar nicht auszumachen. Vielmehr ergibt sich die Funktionalität der Berechnung im Allgemeinen aus dem Zusammenspiel sämtlicher Parameter, die deshalb gemeinsam zu betrachten sind. Aber auch eine Auskunft über sämtliche für einen Techniker gespeicherten Parameter, wie z.B.

- Parameter 1 (ehemals Fixkosten je Tour): 1,00
- Parameter 2 (ehemals Fixkosten je Auftrag): 55,00
- Parameter 3 (ehemals Kosten je Km): 0,95
- Parameter 4 (ehemals Kosten je Stunde): 5,00
- Parameter 5 (ehemals Extrakosten je Überstunde): 52,50
- Parameter 6 (ehemals Kosten je Übernachtung): 212,00
- Parameter 7 (ehemals Fahrgeschwindigkeit): 80
- Parameter 8 (ehemals Arbeitsgeschwindigkeit): 150

wird dem Betroffenen kaum weiterhelfen, solange er den Algorithmus und damit das Zusammenspiel der Parameter nicht kennt.

Hier setzt sich das Problem fort. Wie kann man Betroffenen erläutern, wie der Algorithmus arbeitet? Und wer kann das tun? Die ABC AG, die das Tourenplanungssystem einsetzt, kennt den Algorithmus vielleicht selber gar nicht, und der Systemanbieter verrät nichts, weil er das mühsam ausgetüftelte Rechenverfahren als sein Betriebsgeheimnis betrachtet. Ein spezieller Fall liegt vor, wenn dem eingesetzten Algorithmus ein neuronales Netz zu Grunde liegt, das zuvor an Beispielen trainiert wurde und dessen Verhalten von möglicherweise Tausenden „erlernter" Sensitivitätsparameter zwischen 0 und 1 an den Synapsen gesteuert wird. Dann kann tatsächlich niemand, auch nicht der Systembetreiber, erklären, wie der Algorithmus im Einzelfall funktioniert. Aber selbst wenn der Algorithmus der verantwortlichen Stelle bekannt wäre, würde es ihr normalerweise schwerfallen ihn bei einem Auskunftsersuchen so zu beschreiben, dass der Betroffene, vielleicht ein Informatik-Laie, das Berechnungsverfahren in allen wesentlichen Aspekten versteht.

Wenn man – wie oben erwogen – unter Richtigkeit eines Parameters oder einer gemeinsam wirkenden Gruppe von Parametern die Eignung für die Berechnung eines richtigen Ergebnisses, im Falle der Tourenplanung eines optimalen Tourenplans versteht, kommen zwei weitere Schwierigkeiten dazu. Zum einen kann die Suboptimalität eines Tourenplans neben ungeschickt gewählten Parametern noch ganz andere Gründe haben, z.B. schlicht einen mangelhaften Algorithmus. Zum andern wäre zu klären, was „optimal" eigentlich heißen soll. Die Beurteilung des Ergebnisses ist in vielen Fällen subjektiv.

Transparenz über personenbezogene Auswertungen nach der DSGVO

Die in der DSGVO verankerten Informations- und Korrekturrechte der Betroffenen richten sich primär auf Umfang und Inhalt der gespeicherten Daten und auf ihre Weitergabe. Zur Information über die Auswertungen personenbezogener Daten enthält die DSGVO im Grunde nur eine einzige Regelung, die auch nur in besonderen Fällen greift.[2] Sie gilt nämlich nur dann, wenn die betroffene Person *„einer ausschließlich auf einer automatisierten Verarbei-*

tung beruhenden Entscheidung unterworfen [wird], die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt" [Art. 22 Abs. 1 DSGVO] oder wenn die Entscheidungen auf besonderen Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO beruhen, also auf Daten über die Gesundheit, sexuelle Orientierung, religiöse Überzeugungen usw. [Art. 22 Abs. 4 DSGVO]. In diesen Fällen haben die Betroffenen ein Recht auf *„aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person"* [gem. Artt. 13 Abs. 2 lit. f und 14 Abs. 2 lit. g DSGVO bei der Datenerhebung bzw. gem. Art. 15 Abs. 1 lit. h DSGVO bei einem Auskunftsersuchen der Betroffenen].

Ob unsere oben betrachteten Beispiele für die Auswertung personenbezogener Daten die Voraussetzungen für den Informationsanspruch der Betroffenen auslösen, ist nicht offensichtlich. So können die errechneten Touren bei der ABC AG nachträglich sozusagen von Hand verändert werden, über die Kreditvergabe und die Einstellung von Stellenbewerbern entscheidet letztlich ein Mensch. Und wenn jemand aufgrund seiner Surf-Spuren im Internet bestimmte Werbung erhält, führt das nicht unbedingt zu einer Beeinträchtigung, die einer rechtlichen Wirkung vergleichbar wäre. Weil die automatisch erzielten Berechnungsergebnisse aber in der Praxis prägenden Einfluss auch auf die menschlichen Entscheidungen haben und weil die Grenzen zwischen Belästigung und Beeinträchtigung fließend sind, sollten die Voraussetzungen für die Informationspflicht weiter gefasst werden. Wie weit, wäre eine ausführlichere Betrachtung wert, bei der man – analog zu den Daten – eine uneingeschränkte Informationspflicht nicht ausschließen sollte.

Der Inhalt der Auskunftspflicht bleibt mit der Formulierung über die „involvierte Logik" der Verarbeitung unscharf. Inwieweit sich die „involvierte Logik" vom eigentlichen Algorithmus unterscheidet, ob ihre Darstellung vielleicht gröber sein kann als die des Algorithmus selbst und wann man Informationen darüber „aussagekräftig" nennen kann, bleibt offen. Bemerkenswert ist allerdings die Pflicht zur Information auch über die „Tragweite und die angestrebten Auswirkungen" für die Betroffenen, weil damit jenseits der technisch-operativen Abläufe eines Auswertungsalgorithmus wichtige pragmatische Aspekte des Anwendungskontextes dargestellt werden müssen.

Ein direktes Pendant zum Korrekturanspruch bei unrichtigen Daten kennt die DSGVO im Hinblick auf „unrichtige" Algorithmen nicht. In manchen Fällen aber garantiert sie den Betroffenen – wiederum auf der Ebene des Anwendungskontextes – *„das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung"* [Art. 22 Abs. 3 DSGVO], so dass die Betroffenen zumindest eine Chance haben die auf dem Algorithmus fußende Entscheidung zu beeinflussen.

Fazit

Wir stellen zusammenfassend fest:

1. Einige IT-Systeme verarbeiten personenbezogene Daten, die für sich genommen, also auf der semantischen Ebene, keine Bedeutung haben, deren pragmatische Bedeutung aber darin liegt, wie sie als Eingabeparameter Algorithmen und deren Ergebnisse beeinflussen. Die Berechnungsergebnisse solcher Systeme können für die Betroffenen von hoher Relevanz sein. Selbst wenn die Parameter eines Programms eine semantische Bedeutung haben, kommt meist eine wichtige pragmatische Bedeutung dazu.
2. Um die gebotene Transparenz für die Betroffenen zu schaffen, muss auch über die pragmatische Bedeutung der über sie gespeicherten Daten Auskunft erteilt werden, d.h. über die eingesetzten Algorithmen und ihre Nutzung.
3. Auskunft über die Algorithmen zu erteilen, stößt – zumindest in den interessanten, nicht-trivialen Fällen – auf massive Schwierigkeiten. Diese liegen in der Komplexität bei zugleich fehlenden Methoden für eine leicht verständliche Darstellung der Zusammenhänge, bei „lernenden" Algorithmen in der systematisch bedingten Undurchschaubarkeit, manchmal auch im Rechtsschutz für Betriebsgeheimnisse.
4. Die Richtigkeit von Daten auf der pragmatischen Ebene ist im Allgemeinen nicht objektiv, oftmals auch gar nicht zu bestimmen. Ein Korrekturanspruch ist schon konzeptionell schwer zu fassen.

Was folgt daraus? Die Tatsache, dass für die Wahrung der Persönlichkeitsrechte nicht nur die Verfügbarkeit personenbezogener Daten in IT-Systemen kritisch ist, sondern erst recht die Art ihrer Auswertung und weiteren Verwendung, ist eigentlich offenkundig. Man muss ihr aber im Hinblick auf das Transparenzgebot samt Auskunfts- und Korrekturanspruch mehr Aufmerksamkeit schenken und auch tatsächlich viel mehr Rechnung tragen. Dass eine in diesem Sinne umfassendere Auskunftserteilung schwierig ist, ändert nichts an ihrer Erforderlichkeit.

Schon die konventionelle Einzelauskunft über gespeicherte Daten und ihren Inhalt ist oft wegen der großen Datenmengen schwierig. Doch auch hier gilt der Anspruch auf vollständige Auskunft ohne Einschränkungen. In der Praxis hilft sowohl der verantwortlichen Stelle als auch den Betroffenen eine gestufte Vorgehensweise, bei der in einem ersten Schritt zur Orientierung relativ grobe Datenkategorien beschrieben werden, während eine Information im Detail erst in einem zweiten Schritt folgt, nachdem der Betroffene den Schwerpunkt seines Auskunftsinteresses eingrenzen konnte. Eine ähnliche Stufung vom Groben zu den Einzelheiten könnte die Schwierigkeiten auch bei der Auskunft über die Auswertung der Daten lindern.

Wie bei den Daten darf es eine Verweigerung der Auskunft zur Funktionalität der Algorithmen – notfalls auch im Detail – nicht geben. Das gilt zumindest dann, wenn die Verarbeitung der personenbezogenen Daten einen maßgeblichen Einfluss auf unmittelbare Folgen für die Betroffenen hat, sei es ein Dienst- oder Tourenplan, sei es ein Kreditangebot. Dann müssen die Algorithmen auf Anfrage offengelegt werden. Verantwortliche Stellen können sich nicht dadurch aus der Affäre ziehen, dass ein Dienstleister die Be-

rechnungen ausführt und die Verfahren nicht bekanntgibt. Die verantwortliche Stelle bleibt verantwortlich und muss auskunftsfähig bleiben. Sie darf solche „geheimnisvollen" Dienstleister dann nicht beauftragen. Auch sie selbst darf keine per se intransparenten Verfahren etwa auf der Basis von neuronalen Netzen einsetzen. Für kritische Entscheidungen müssen undurchschaubare Algorithmen tabu sein.

Selbst bei bestem Willen bleibt es objektiv schwierig die Arbeitsweise oftmals raffinierter Algorithmen verständlich zu beschreiben. Auch bei einer schrittweisen Verfeinerung der Auskunft von groben Systemkomponenten über Funktionsblöcke zu Einzelfunktionen wird es nicht jedem Betroffenen möglich sein die für ihn wesentlichen Aspekte des Programmablaufs zu verstehen also insbesondere die Kriterien für die Berechnung einer Entscheidungsempfehlung zu erkennen und ihre Wichtung möglicherweise als unangemessen anzugreifen. Der Anspruch auf Transparenz über die Technik ist deshalb aber nicht obsolet. In wichtigen Fällen können betroffene Laien die Hilfe von Fachleuten in Anspruch nehmen. Das ist in vielen anderen Zusammenhängen gang und gäbe. Man fragt Rechtsanwälte, Steuerberater, Automechaniker und Ärzte, wenn man Zusammenhänge selbst nicht überschaut. Standard-Algorithmen können in der Fachöffentlichkeit untersucht, beschrieben und beurteilt und für die allgemeine Öffentlichkeit erläutert werden, wie es zum Beispiel bei Verschlüsselungsverfahren geschieht.

Der in der DSGVO angelegte Ansatz Transparenz und Selbstbestimmung auf der Ergebnisseite zu stützen, bleibt gut und richtig. Der Anspruch darauf die Ergebnisse der Berechnungen zu erfahren, gegenüber einem Menschen kommentieren und wo möglich die abzuleitenden Konsequenzen zu beeinflussen, sollte sogar eher die Regel als die Ausnahme in eng umgrenzten Sondersituationen sein. Ein Bankkunde sollte eine Chance haben die Verhandlungen über Kreditkonditionen mit inhaltlich vernünftigen Argumenten auszuhandeln, egal, auf welchen Wegen irgendein Bonitäts-Score errechnet wurde. Ein Außendienst-Techniker sollte nicht nur ein Mitspracherecht über die Eingabeparameter Arbeitsgeschwindigkeit und Reisegeschwindigkeit haben, sondern er sollte jeden errechneten Tourenplan ablehnen, mit dem Disponenten unter verschiedensten inhaltlichen Gesichtspunkten diskutieren und einvernehmlich ändern können. Schließlich geht es bei den Berechnungsergebnissen oft nicht so sehr um richtig oder falsch, sondern eher um Fairness, und die können die meisten Betroffenen auch ohne Informatik-Kenntnisse kompetent beurteilen.

1 Allein die Minimierung der Fahrstrecke ist in der Informatik unter dem Begriff des Travelling-Salesman-Problems bekannt und anerkanntermaßen als hoch komplex einzustufen.

2 Bemerkenswerterweise sieht die DSGVO im Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 nur Angaben zu den verarbeiteten Datenkategorien, zu Datenempfängern und Löschfristen vor, nicht aber zu den Auswertungen oder Verknüpfungen der Daten.

Heinz Alenfelder

Gedanken zum Datenschutz für „nicht mehr beschäftigte" Rentner:innen

Irgendwann ist es soweit: Aus dem Beschäftigtenstatus wird – mehr oder weniger schnell – der des Status „In Rente". Zwar müssen bzw. dürfen einige Daten aus dem alten Beschäftigungsverhältnis beim Arbeitgeber verbleiben, doch tun sich durchaus neue Problemfelder für die Renter:innen auf. Einige praktische Aspekte sollen im folgenden Text zumindest angerissen werden.

Dienstliche E-Mails, Netzwerk und Webseite des Arbeitgebers

Mit dem Ende des Arbeitsverhältnisses endet die Zugehörigkeit zum Betrieb des Arbeitgebers und damit in der Regel die Gültigkeit einer entsprechenden E-Mail-Adresse. Der Arbeitgeber behält das Recht an den dienstlichen E-Mails, unabhängig von der Erlaubnis die E-Mail-Adresse auch für private Zwecke nutzen zu können. Alle privaten E-Mails und E-Mail-Kontakte können und sollten also vor dem Ende des Arbeitsverhältnisses gelöscht werden. Außerdem empfiehlt es sich eine private E-Mail-Adresse an diejenigen Kolleg:innen weiterzugeben, mit denen ein Austausch weiterhin gewünscht ist. Wenn seitens des Betriebs eine aktive Ehemaligen-Betreuung stattfindet, muss der dabei stattfindenden Datenverarbeitung personenbezogener Daten getrennt zugestimmt werden.

Zum Abschied ist auch die Frage zu stellen, ob der Account bei einem der auf berufliche Kontakte ausgerichteten sozialen Netzwerke, wie Xing oder LinkedIn, bestehen bleiben soll – und vor allem mit welchen Informationen die Besucher:innen der dortigen Seite in Zukunft versorgt werden. Darüber hinaus ist es durchaus sinnvoll die Webseite des (früheren) Arbeitgebers daraufhin zu überprüfen, ob der eigene Name dort noch auftaucht, etwa bei den „Teammitgliedern".

Private E-Mails, soziale Netzwerke und Kontakte

Mit dem Ablauf der dienstlichen E-Mail-Adresse – so dachte und hoffte manch ein:e Pensionär:in vielleicht –

wird auch der Zufluss der Spam-Mails versiegen. Weit gefehlt: Ab jetzt gibt es keine:n Administrator:in mehr, der oder die dafür sorgen kann, dass die Mailbox sauber bleibt. Oft muss das E-Mail-Programm „trainiert" werden, so dass es Spam-Mails automatisch in einen speziellen Ordner ablegt oder sofort löscht. Außerdem ist zu überlegen, ob sich das Anlegen mehrerer privater E-Mail-Adressen lohnt, die dann für die verschiedenen Interessenbereiche genutzt werden. Der E-Mail-Dienst posteo.de (siehe auch DANA 1/2022 S. 11 ff.) bietet standardmäßig drei E-Mail-Adressen für den Basisaccount und weitere gegen einen kleinen Aufpreis an. Bei konsequenter Zuordnung der Adressen kann auch die Spam-Häufigkeit getrennt betrachtet werden. Hoffentlich wächst in diesem Feld im Laufe der Zeit das Serviceangebot für die älteren Generationen.

Soziale Kontakte können nach dem Ende aller Beschäftigungsverhältnisse intensiviert werden. Hier heißt es dann allerdings ganz stark zu bleiben, wenn die jeweilige „Community" statt zum Telefon zu greifen Termine nur noch über Doodle oder in der WhatsApp-Gruppe absprechen will. Selbst wenn bisher die Zeit dafür gefehlt hat, wäre jetzt ein Umstellen und eine intensive Werbung für Alternativen wie nuudel, Signal oder Threema angebracht. Gerade diejenigen, denen im Beschäftigungsverhältnis der Aufwand zu groß war sich mit alternativer Software auseinanderzusetzen, sind jetzt berufen sich zu informieren und vielleicht sogar Beratung für ihre Freund:innen anzubieten.

Das Rentner:innen-Dasein lässt bekanntlich Zeit für Vieles. Wer jetzt etwa daran geht eine Münz- oder Briefmarkensammlung zu starten oder auch eine früher begonnene Sammlung zu vervollständigen, erliegt vielleicht der Werbung, die sich speziell an die älteren Generationen richtet: Vom Treppenlift über Goldmünzen und -medaillen bis zu verschreibungsfreien Medikamenten und „Kaffeefahrten" – all dies wird beworben. Es kann ganz einfach nicht nur über das Internet, sondern weiterhin per Post – oft zur Probe mit Rückgaberecht – bestellt werden. Nur ganz, ganz klein gedruckt findet sich in der Regel der Hinweis, dass danach auch der Weiterverarbeitung der Daten widersprochen werden kann. Und wer das nicht tut, muss sich nicht wundern, nach Kündigung des Münzsammelabonnements irgendwann die neueste Erfindung der Hörgeräteakustik angeboten zu bekommen. Hier heißt es: Augen auf noch vor dem Kauf!

Insgesamt bleibt festzustellen, dass mit dem Ende aller Beschäftigungsverhältnisse die Verantwortung für den korrekten Umgang mit den eigenen personenbezogenen Daten viel Arbeit bedeuten kann.

Bereits Wilhelm Busch beschrieb dies eindrucksvoll, als er dichtete:

„Meist in Wagen, die nicht federn,
Selten nur auf Gummirädern
Fährt der Mensch durch diese Welt,
Bis er in den Graben fällt."

Thilo Weichert

TADPF-Datenaustausch mit den USA bleibt „Rohrkrepierer"

Vorausgegangen waren 2000 „Safe Harbor" und 2016 das „Privacy Shield", um einen „rechtssicheren" Datenaustausch Europas mit den USA zu gewährleisten. Diese Konstrukte wurden vom Europäischen Gerichtshof (EuGH) mit seinen Urteilen vom 06.10.2015[1] und vom 16.07.2020[2] aufgehoben. Das oberste europäische Gericht stellte jeweils fest, dass die Beschlüsse der Europäischen Kommission, die den Datentransfer von Europa in die USA erlaubten, wenn sich die US-Firmen einer Selbstzertifizierung unterwerfen, gegen die europäische Grundrechte-Charta verstießen, insbesondere gegen das dort in Art. 8 garantierte Grundrecht auf Datenschutz und die Rechtsschutzgarantie in Art. 47. Gründe für diesen Verstoß sah der EuGH viele: Es besteht in den USA kein den europäischen Standards entsprechendes Datenschutzrecht. Besonders problematisch ist, dass – wie Edward Snowden 2013 offenlegte – US-Behörden verdachtsunabhängig Massendaten abschöpfen und diese u.a. für Geheimdienst- und Sicherheitszwecke nutzen. Eine unabhängige Datenschutzaufsicht ist nicht gesichert, ebenso wenig die Transparenz für die Betroffenen und die Möglichkeit gegen die unberechtigte Datenverarbeitung vor einem unabhängigen Gericht vorzugehen. Die Aufhebung von Safe Harbor und Privacy Shield hatte jeweils der Datenschutzaktivist Max Schrems – mittlerweile von der Organisation noyb[3] – beim EuGH erstritten, zum Unbehagen der EU-Kommission, der US-Regierung und vieler US-Firmen, die Daten von Europäern in den USA verarbeiten – allen voran IT-Großkonzerne. Von diesen Datentransfers betroffen sind Daten von Social-Media-Anbietern, etwa von Meta (Facebook, WhatsApp, Instagram), Suchmaschinen (Bing, Google Search), Cloud-Dienstleistern wie Salesforce oder Amazon Web Services (AWS), Softwareanbietern wie Google, Microsoft oder Apple und Online-Händlern wie Amazon.

Um diesen rechtswidrigen Zustand schnellstmöglich wieder zu beseitigen, hatten sich EU-Kommissionspräsidentin Ursula von der Leyen und US-Präsident Joe Biden im März 2022 darauf verständigt eine neue Vereinbarung zum Datentransfer abzuschließen.[4] Mehr als sechs Monate später gab Biden bekannt, er habe eine „Exekutive Order"[5] unterzeichnet, mit der die US-Massenüberwachung eingeschränkt und rechtliche Gegenwehr hiergegen ermöglicht werde. Diese Verwaltungsanordnung soll nach dem Willen der EU-Kommission zentraler Bestandteil eines neuen Angemessenheitsbeschlusses zum Datentransfer sein. Es werde ein


Bild: iStock.com / Rawf8

sicherer Datenfluss und angemessener Datenschutz gemäß den EuGH-Vorgaben auf einer dauerhaften und verlässlichen Rechtsgrundlage gewährleistet. Der Name des Abkommens wurde – sperriger als zuvor – auf „Trans-Atlantic Data Privacy Framework“ (TADPF) festgelegt. Für viele ist das TADPF aber nichts anderes als ein Safe Harbor III oder ein Privacy Shield II. Ende 2022 soll das Abkommen stehen.[6]

Betrachtet man den neuen Rechtsrahmen genauer, so erweist sich dieser als nicht viel mehr als ein erneuter Etiketten-Schwindel. Geändert werden weniger die Inhalte als die Begriffe: Die Massenüberwachung durch US-Geheimdienste, allen voran durch die National Security Agency (NSA), soll nicht mehr „maßgeschneidert“, sondern „verhältnismäßig“ und „notwendig“ sein. An der Praxis soll sich – soweit ersichtlich – nichts ändern. Und genau diese wurde vom EuGH als unverhältnismäßig verworfen. Mit der durch Art. 47 der Grundrechtecharta geforderten Rechtsbehelfsmöglichkeit wird ähnlich leichtfertig umgegangen: Für die Rechtskontrolle soll ein „Data Protection Review Court“ zuständig sein. Dabei handelt es sich aber nicht – was der Begriff nahelegt – um ein unabhängiges Gericht, sondern um eine Verwaltungseinrichtung, die den früheren Ombudsman ersetzen soll. Die Prüfung des „Courts“ soll auch nicht in eine für die Beschwerdeführer transparente Entscheidung münden, sondern in die karge Aussage, dass keine Datenschutzverletzung festgestellt wurde – oder vielleicht doch.

Noch nicht im Ansatz erkennbar ist, dass und wie die Forderungen nach Zweckbindung und nach Betroffenenrechten bei den sich selbst zertifizierenden Unternehmen gesichert sein werden. Die Grundsätze des TADPF entsprechen den veralteten von Safe Harbor und bleiben weit hinter der DSGVO zurück. Versuche, das US-Datenschutzrecht nach europäischem Vorbild zu verbessern, gab es schon einige. Doch selbst das als fortschrittlichstes US-Gesetz gepriesene Recht in Kalifornien bleibt in wesentlichen Fragen – z.B. beim Auskunftsanspruch – weit hinter EU-Standards zurück. Dies gilt auch für die Datenschutzaufsicht, die weder unabhängig noch Rechtsschutz gewährend ausgestaltet ist. Die Gründe hierfür liegen tief, da die US-Verfassung, die US-Einwohnern nur einen reduzierten Datenschutz gewährt, für europäische Betroffene überhaupt keine Garantien gibt.[7]

Max Schrems hat schon angekündigt, dass er auch einen TADPF-Beschluss der EU-Kommission angreifen wird.[8] Ändert sich an dem absehbaren TADPF-Rahmen nichts massiv und auch nichts an der Position des EuGH – beides ist nicht absehbar – dann wird auch der neue Beschluss aufgehoben werden.

Was bedeutet dies nun für die Verarbeitung von Daten in den USA? Zunächst ist offensichtlich, dass weiterhin keine Rechtssicherheit besteht. Am zuverlässigsten für eine konzerninterne Datenverarbeitung wären verbindliche Unternehmensrichtlinien (Binding Corporate Rules – BCR), die nicht von der EU-Kommission, sondern von den Aufsichtsbehörden zu genehmigen sind (Art. 47 DSGVO). Diesen Weg gehen einige, vor allem europäische Konzerne.[9] Ein Vorteil der BCR liegt darin, dass sie weltweit angewendet werden können. Praktisch alle großen US-Konzerne nutzen derzeit keine BCR. Der Grund ist banal und zugleich entlarvend: Diese müssten sich gegenüber der unabhängigen Datenschutzaufsicht ausdrücklich auf verbindliche Datenschutzstandards verpflichten. Das wollen Meta, Alphabet & Co. nicht – trotz allem von ihnen verbreiteten Datenschutzgesäusel.

Sie verwenden sog. Standarddatenschutzklauseln. Diese hat der EuGH in seiner Schrems-II-Entscheidung nicht grundsätzlich verworfen. Wohl aber hat das Gericht klargestellt, dass in den Anhängen zu den Klauseln konkret benannt werden muss, durch welche technisch-organisatorischen Maßnehmen und vor allem durch welche verfahrensmäßigen Vorkehrungen ein angemessenes Datenschutzniveau geschaffen wird. Die bisher durchgängig verwendeten salbungsvoll klingenden, aber allgemein bleibenden Zusicherungen genügen jedenfalls nicht.

Eine in die richtige Richtung gehende Problemlösung kann auch darin bestehen, dass die Datenverarbeitung des US-Unternehmens räumlich in der EU erfolgt. So sind etwa entsprechende Zusicherungen von AWS, Google oder Microsoft möglich. Dadurch wird der Zugriff von US-Behörden erschwert, auch wenn er nicht völlig ausgeschlossen ist: Im US-Recht ist vorgesehen, dass in den USA ansässige Unternehmen wie auch deren Töchter in Europa verpflichtet werden können auch ihre in der EU gespeicherten Daten herauszugeben – so der Foreign Intelligence Surveillance Act (FISA), der Patriot Act und der CLOUD-Act. Daher sind entsprechende Zusicherungen mit einem Verfahren zu hinterlegen, das die Überprüfung eventuell erfolgender Datenherausgaben ermöglicht. Die Rechtsprechung der nationalen Gerichte zur Datenverarbeitung durch US-Unternehmen in Europa ist noch völlig uneinheitlich.[10]

Der weitere Ablauf ist absehbar: Die Europäische Kommission wird das TADPF als angemessen i.S.v. Art. 45 DSGVO beschließen, obwohl der Europäische Datenschutzausschuss davon abrät. Es wird erneut zu einer Prüfung durch den

EuGH kommen – was wieder mindestens zwei Jahre dauern wird. Während dieser Zeit wird die Datenübermittlung in die USA auf der TADPF-Grundlage wieder als zulässig fingiert; danach wird diese Fiktion wieder beseitigt sein. Vielleicht hat sich bis dahin der EuGH zu seinen spezifizierten Anforderungen an die Umsetzung der Standarddatenschutzklauseln geäußert. Klarheit haben bis dahin einige Konzerne dadurch hergestellt, dass sie sich ihre BCR haben genehmigen lassen. Die Masse der US-Konzerne aber wird weiterhin ein illegales Geschäftsmodell mit einer Verarbeitung in den USA betreiben…

1 EuGH U.v. 06.10.2015 – C-362/14 (Safe Harbor, Schrems I).

2 EuGH U.v. 16.07.2020 – C-311/18 (Privacy Shield, Schrems II).

3 none of your business, https://noyb.eu/de.

4 Joint Statement on Trans-Atlantic Data Privacy Framework, https://ec.europa.eu/commission/presscorner/api/files/document/print/nl/ip_22_2087/IP_22_2087_EN.pdf.

5 https://noyb.eu/sites/default/files/2022-10/Biden%20EO%20on%20Surveillance%2C%20Structured.pdf.

6 European Commission, Questions & Answers: EU-U.S. Data Privacy Framework, 07.10.2022, https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045.

7 Siehe auch die Kritik von noyb, Erste Reaktion: Executive Order zur US-Überwachung reicht wohl nicht, 07.10.2022, https://noyb.eu/de/executive-order-zur-us-ueberwachung-reicht-wohl-nicht.

8 Trans-Atlantic Data Privacy Framework: Bald Schrems-III? 13.10.2022, https://www.dr-datenschutz.de/trans-atlantic-data-privacy-framework-bald-schrems-iii/.

9 Die Liste der Unternehmen ist veröffentlicht unter https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en.

10 Siehe dazu z.B. Vergabekammer Karlsruhe v. 13.07.2022 einerseits und OLG Karlsruhe v.07.09.2022 andererseits, beides in diesem Heft, S. 283.

Presseerklärung der DVD vom 06.09.2022

DVD: „Wissings Digitalstrategie ist ein wert(e)loser Ankündigungskatalog“

Die Deutsche Vereinigung für Datenschutz e.V. (DVD) hat mit Erschrecken die am 31.08.2022 von Digitalminister Volker Wissing vorgelegte, so genannte Digitalstrategie der Bundesregierung zur Kenntnis genommen. Diese beschränkt sich darauf die im rot-grün-gelben Koalitionsvertrag verstreuten Absichtsbekundungen zu wiederholen und macht hierzu gar einige wesentliche Abstriche.

Erschreckt ist die DVD über das, was in der Digitalstrategie nicht enthalten ist: Zwar werden Grundrechte und Datenschutz floskelhaft immer wieder erwähnt, doch von einer „Strategie“ eines digitalen Grundrechtsschutzes ist nichts zu erkennen, ebenso wenig, dass hieran in der neuen Bundesregierung gearbeitet wird. So wird etwa ein Beschäftigtendatenschutzgesetz angekündigt, ja es wird der Eindruck erweckt, das läge schon vor, tatsächlich aber ist das Projekt auf unbefristete Zeit verschoben. Das im Koalitionsvertrag angekündigte Forschungsdatengesetz wird ersetzt durch „Datenzugangsrechte für die Forschung (Forschungsklauseln)“, was den gesetzlichen Flickenteppich vergrößern würde und die Forschungsprivilegierung der Datenschutz-Grundverordnung, die einher gehen muss mit Schutzgarantien, ignoriert. Es wird von einem „gemeinsamen Datenhaus“ einer „digitalen Polizei“ schwadroniert ohne die seit Jahren überfälligen, vom Bundesverfassungsgericht geforderten Schutzmaßnahmen auch nur zu erwähnen, geschweige die im Koalitionsvertrag angekündigte „Überwachungsgesamtrechnung“.

Von der „Zeitenwende“, in der sich die globale Digitalpolitik befindet, ist keine Rede, sondern inhaltslos von einer „digitalen Außenpolitik“: Dass der europäische digitale Grundrechtsschutz mit dem US-amerikanischen ungehinderten Ausbeuten von Kundendaten, den aus Russland kommenden Hackerattacken und der expansiv betriebenen chinesischen Überwachungspolitik vor einer gewaltigen Herausforderung steht, dem strategisch von der europäischen Politik entgegengewirkt werden muss, ist der „Strategie“ keine Erwähnung wert.

DVD-Vorsitzender Frank Spaeing: „So richtig es sein mag, dass angesichts der vielfältigen Krisen und Bedrohungen für das Klima, für den Frieden und die Energieversorgung von der Bundesregierung gerade andere politische Schwerpunkte gesetzt werden, so wenig dürfen die Ministerialverwaltung und die digitalen Fachpolitiker ihre Hausaufgaben vernachlässigen. Das, was Herr Wissing hier vorgelegt hat, lässt nicht im Ansatz erkennen, dass die Regierung mit ihren Hausaufgaben begonnen hat. Es besteht die Gefahr, dass der Stillstand der Merkel-Regierungen bei der werteorientierten Digitalpolitik unter Rot-Grün-Gelb nahtlos fortgesetzt wird.“ Thilo Weichert vom DVD-Vorstand ergänzt: „Folgenlose Ankündigungspolitik haben wir lange genug gehabt. In Wissenschaft, Zivilgesellschaft und in der Wirtschaft besteht das Fachwissen und das strategische Denken, das von der Politik endlich abgerufen werden und zu Umsetzungsaktivitäten führen muss.“

Presseerklärung der DVD vom 04.10.2022

DVD weist Spende aus rechtsmissbräuchlicher Google-Fonts-Abmahnung zurück

Pseudo-Datenschützer instrumentalisieren Bürgerrechtsverein

Am 28. September erreichte die Geschäftsstelle der Deutschen Vereinigung für Datenschutz e.V. (DVD) eine ungewöhnliche E-Mail, in der nach der Kontonummer des DVD-Spendenkontos gefragt wurde. Am nächsten Tag landeten 3060 € eines Martin Ismail aus Hannover auf dem Konto der als gemeinnützig anerkannten Bürgerrechtsorganisation, die sich seit über 40 Jahren für mehr Datenschutz engagiert, verbunden mit einer weiteren E-Mail, man möge bitte eine Spendenquittung ausstellen, so dass diese Spende steuerlich abgesetzt werden kann.

Eine Recherche der DVD ergab, dass sich hinter der „Spende" eine „Interessengemeinschaft Datenschutz" (IG Datenschutz) verbirgt, die sich auf ihrer Webseite https://igdatenschutz.de der DVD-Spende rühmte mit der Behauptung, die DVD verfolge „ein sehr ähnliches Ziel wie die IG Datenschutz, weswegen wir mit Spenden ihr Arbeit unterstützen möchten" (Rechtschreibfehler im Original).

Eine Internetsuche ergab, dass die „IG Datenschutz" sich das überwiesene Geld von hunderten, vielleicht sogar tausenden Webseitenbetreibern erpresst hatte, die – wohl in datenschutzrechtlicher Unkenntnis – auf ihrer Seite Google-Fonts, ein Schriftartenangebot, als Cloud-Angebot eingebunden hatten. Ismail und sein Rechtsanwalt Kilian Lenard aus Berlin mahnen seit August massenhaft Webseitenbetreiber ab und fordern von ihnen z.B. 170 € Schadenersatz dafür, dass durch den Webseitenbesuch die personenbezogenen Daten von Herrn Ismail unzulässigerweise in die USA übermittelt worden seien. Gerechtfertigt wird die Forderung mit einem Gerichtsurteil, das einem Betroffenen in solch einem Fall einen Schadenersatz von 100 € zusprach. Dieses offenbar höchst erfolgreiche Geschäftsmodell versucht die „IG Datenschutz" nun durch publikumswirksame Spenden – nicht nur für die DVD, sondern auch für den „Deutschen Kinderverein e.V." – reinzuwaschen.

Hinter der „IG Datenschutz" verbirgt sich offenbar nichts anderes als der Herr Ismail und sein Berliner Rechtsanwalt mit einigen Mitstreitern. Die DVD reagierte umgehend und teilte der „IG Datenschutz" mit, dass die Spende zurückgewiesen werde. Sie forderte die „IG Datenschutz" auf die ehrverletzende Aussage, die DVD verfolge ein „sehr ähnliches Ziel", umgehend von der Webseite zu beseitigen.

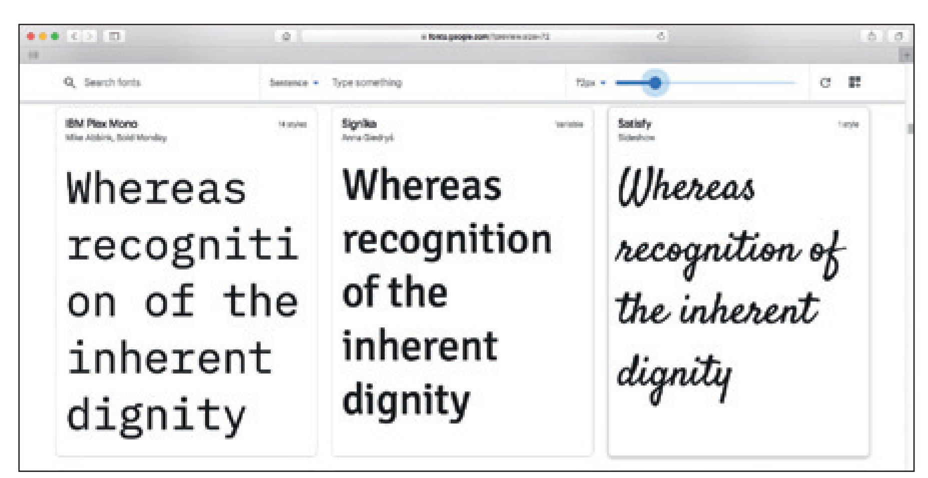
Richtig ist, dass sich die DVD auch im internationalen Datenverkehr mit den USA für das Datenschutzgrundrecht einsetzt und deshalb die rechtlich fragwürdige Einbindung von US-Angeboten auf europäischen Webseiten (wie die besagte Einbindung von Google Webfonts als Cloud-Angebot) kritisiert.

DVD-Vorstandsmitglied Thilo Weichert: „Die DVD lehnt das als erpresserisch empfundene Vorgehen der ‚IG Datenschutz' ab. Hiermit wird das Anliegen des Datenschutzes diskreditiert; getroffen werden ‚die Kleinen' und im konkreten Fall nicht Google, das sich mit dem Schriftartendienst ‚Google Fonts' weltweit auf illegale Weise Daten der Webseitenbesucher besorgt, mit denen sein globales Werbenetzwerk versorgt wird."

DVD-Vorsitzender Frank Spaeing ergänzt: „Wir raten Abgemahnten dringend zu überlegen, ob sie auf die Forderungen des Duos Ismail-Lennard eingehen wollen. Deren Forderungen scheinen rechtsmissbräuchlich. Wir raten aber ebenso den Abgemahnten auf ihrer Webseite die Online-Google-Fonts (sowie alle anderen rechtswidrig eingebundenen Dienste) zu deaktivieren."

Die DVD weist darauf hin, dass die Google Fonts auch lokal eingebunden werden können, wodurch es nicht zu Datenübermittlungen in die USA und zu keiner Ausspionierung der Webseitenbesucher kommt, die Schriftarten aber dennoch genutzt werden können. Anleitungen zum Herunterladen der Fonts finden sich zahlreich im Netz.
(siehe hierzu auch die Meldung in diesem Heft auf S. 276).

Weitere Informationen im Netz zu dem Vorgang finden Sie unter:
- https://www.abofalle-anwalt.de/kilian-lenard-martin-ismail-google-fonts/
- https://www.anwalt.de/rechtstipps/abmahnung-martin-ismail-wegen-datenschutz-204782.html



Meldung in eigener Sache

Registerveröffentlichungen

Am 15.08.2022 veröffentlichte die Deutsche Vereinigung für Datenschutz (DVD) eine Presseerklärung „Online-Registerveröffentlichungen verstoßen gegen Datenschutz“, die auch in der DANA 3/2022, 177 (siehe auch die Meldung DANA 3/2022, 178) abgedruckt ist. Unsere Erklärung führte zu vielen Rückmeldungen – vor allem von Betroffenen, die sich gegen die Veröffentlichung ihrer sensiblen Daten im zentralen Vereinsregister oder Handelsregister zur Wehr setzen wollen. Der DVD geht es darum eine grundsätzliche Lösung zu finden, wozu alle politisch und rechtlich Verantwortlichen (Bund, Landesregierung Nordrhein-Westfalen, Amtsgericht Neuss, Amtsgerichte generell, Notare) bisher nicht bereit zu sein scheinen.

Die DVD kümmert sich weiterhin um das Problem, das sich aber als rechtlich äußerst komplex erweist. Über die Aktivitäten berichten wir auf unserer Webseite www.datenschutzverein.de.

Offener Brief gegen Chatkontrolle

114 europäische und internationale Organisationen haben sich in einem offenen Brief an die EU-Kommission gegen die Pläne zur Chatkontrolle gewandt.

Sehr geehrte EU-Kommissar.innen,

wenn Sie die Funktionsweise des Internets grundlegend untergraben, machen Sie es für alle weniger sicher.

Wir schreiben Ihnen als 114 zivilgesellschaftliche Organisationen und Gewerkschaften, die in den Bereichen Menschenrechte, Medienfreiheit, Technologie und Demokratie im digitalen Zeitalter tätig sind. Gemeinsam fordern wir Sie auf die „Verordnung zur Festlegung von Vorschriften zur Verhütung und Bekämpfung des sexuellen Missbrauchs von Kindern” (CSA-Verordnung) zurückzuziehen und eine mit den europäischen Grundrechten vereinbare Alternative vorzulegen.

Es ist nicht möglich privat und sicher zu kommunizieren und zugleich einen direkten Zugriff für Regierungen und Unternehmen einzurichten. Auch böswilligen Akteur.innen würden die Maßnahmen Tür und Tor öffnen. Eine sichere Internet-Infrastruktur, die freie Meinungsäußerung und Selbstbestimmung fördert, ist nicht möglich, wenn Internetnutzer.innen einer allgemeinen Überprüfung und Filterung unterzogen werden können und ihnen Anonymität verweigert wird.

Die vorgeschlagene CSA-Verordnung stuft Scanning- und Überwachungstechnologien – trotz gegenteiliger Expert.innenmeinungen – politisch als sicher ein. Sollte dieses Gesetz verabschiedet werden, wird das Internet in einen Raum verwandelt, *der die Privatsphäre, die Sicherheit und die freie Meinungsäußerung aller Menschen gefährdet*.[1] Dies gilt insbesondere für Kinder und Jugendliche, die mit dieser Verordnung eigentlich geschützt werden sollen.

Die vorgesehenen Vorschriften würden Anbieter.innen sozialer Medien für die von ihren Nutzer.innen geteilten privaten Nachrichten haftbar machen. Das würde Plattformen dazu zwingen riskante und fehleranfällige Techniken anzuwenden, *um jederzeit Kontrolle darüber zu haben, was wir alle tippen und teilen*. In der Folgenabschätzung, die dem Verordnungsvorschlag beigefügt ist, werden Unternehmen angehalten Client-Side-Scanning einzusetzen, um ihre Nutzer.innen zu überwachen, wohl wissend, dass die Diensteanbieter.innen das aus Sicherheitsgründen skeptisch sehen. Die Verordnung wäre ein noch nie dagewesener Angriff auf das Recht auf private Kommunikation und die Unschuldsvermutung.

Nicht nur Erwachsene sind auf Privatsphäre und Sicherheit angewiesen. Wie die Vereinten Nationen und UNICEF erklären, ist die Privatsphäre im Netz für die Entwicklung und Selbstverwirklichung junger Menschen von entscheidender Bedeutung. Sie sollten keiner Massenüberwachung ausgesetzt werden. Auch das britische Royal College of Psychiatrists weist darauf hin, dass es für Kinder schädlich ist sie auszuspionieren und dass Maßnahmen, die auf Selbstbefähigung und Bildung basieren, sie im Netz wirkungsvoller schützen.

Die CSA-Verordnung wird in vielerlei Hinsicht schweren Schaden anrichten:

- Eine private Nachricht über die eigene Missbrauchserfahrung, die für einen vertrauenswürdigen Erwachsenen gedacht ist, könnte automatisch markiert, von den Mitarbeiter.innen eines Social-Media-Unternehmens geprüft und dann zur Untersuchung an die Strafverfolgungsbehörden weitergeleitet werden. Das geschähe gegen den Willen der Betroffenen und verletzt ihre Würde. Das könnte Opfer davon abhalten sich Hilfe zu holen;
- Whistleblower.innen und Quellen, die anonym über Korruption in der Regierung berichten wollen, könnten sich nicht mehr auf Online-Kommunikationsdienste verlassen, da die Ende-zu-Ende-Verschlüsselung ausgehebelt wäre. Bemühungen Machthaber.innen zur Rechenschaft zu ziehen, würden erheblich erschwert;
- Private intime Fotos jung aussehender Erwachsener, die diese rechtmäßig an ihre Partner.innen schicken, könnten von der KI fälschlich markiert werden,

Mitarbeiter.innen sozialer Medien angezeigt werden und dann an Strafverfolgungsbehörden geleitet werden;
- Solche unvermeidlichen Falschmeldungen würden Strafverfolgungsbehörden überlasten, die bereits jetzt nicht über die Ressourcen verfügen alle Fälle zu bearbeiten. Sie müssten ihre begrenzten Kapazitäten darauf verwenden riesige Mengen rechtmäßiger Kommunikation zu sichten anstatt gefundenes Missbrauchsmaterial zu löschen und Verdächtige und Täter.innen zu verfolgen;
- Bisher sichere Messengerdienste, zum Beispiel Signal, wären gezwungen ihre Dienste technisch unsicher zu machen. Nutzer.innen hätten dann keine sichere Alternative mehr. Dies würde alle gefährden, die sich auf sichere Kommunikation verlassen: Anwältinnen, Journalisten, Menschenrechtsverteidigerinnen, NGO-Mitarbeiter – einschließlich derer, die Opfern helfen –, Regierungsmitglieder und viele andere. Wenn Dienste die Nachrichten weiterhin verschlüsseln wollen, würden sie mit einer Geldstrafe in Höhe von sechs Prozent ihres weltweiten Umsatzes belegt oder gezwungen sich aus dem EU-Markt zurückzuziehen;
- Quellenschutz und die digitale Sicherheit von Journalist.innen werden gefährdet, weil damit Ende-zu-Ende-Verschlüsselung abgeschafft würde. Außerdem wird die Pressefreiheit durch den „Chilling Effect" der Maßnahmen eingeschränkt;
- Sobald diese Technologie eingeführt wäre, könnten Regierungen auf der ganzen Welt Unternehmen gesetzlich dazu verpflichten nach Beweisen für politische Opposition zu suchen, nach Aktivist.innen, gewerkschaftlichen Zusammenschlüssen und auch nach Menschen, die abtreiben lassen, wo Abtreibung kriminalisiert ist – also nach allem, was eine Regierung womöglich unterdrücken möchte;
- Bereits entrechtete, verfolgte und marginalisierte Gruppen auf der ganzen Welt wären von diesen Bedrohungen besonders betroffen.

In den vergangenen Jahren ist die EU zum Vorreiter für das Menschenrecht auf Privatsphäre und Datenschutz geworden und hat damit einen weltweiten Standard gesetzt. Doch mit der vorgeschlagenen CSA-Verordnung macht die Europäische Kommission eine Kehrtwende in Richtung Autoritarismus, Kontrolle und Zerstörung der Freiheit im Netz. Dies wäre ein gefährlicher Präzedenzfall für weltweite Massenüberwachung.

Zum Schutz der freien Meinungsäußerung, der Privatsphäre und der Sicherheit im Internet fordern wir, die unterzeichnenden 114 Organisationen, Sie als Mitglieder der Kommission auf die Verordnung zurückzuziehen.

Wir fordern stattdessen zielgerichtete, rechtmäßige und technisch machbare Alternativen, um das schwerwiegende Problem des Missbrauchs von Kindern zu bekämpfen. Maßnahmen müssen der Selbstverpflichtung der EU „Digitalen Dekade" zu einem „sicheren und geschützten" digitalen Umfeld für alle entsprechen – das schließt Kinder und Jugendliche ausdrücklich ein.

Unterzeichnende:

Acces Now – International – Alternatif Bilisim (AiA-Alternative Informatik Gesellschaft) – International – Agora Association – Türkei – APADOR-CH – Rumänien – ApTI Romania – Rumänien – ArGE Tübingen – Deutschland – ARTICLE19 – International – Aspiration – Vereinigte Staaten – Associação Portuguesa para a Promoção da Segurança da Informação (AP2SI) – Europa – Association for Support of Marginalized Workers STAR-STAR Skopje – Republik Nordmazedonien – Attac Austria – Österreich – Aufstehn.at – Österreich – Arbeiterkammer Österreich – Österreich – Berlin Strippers Collective – Deutschland – Big Brother Watch – Vereinigtes Königreich – Bits of Freedom – Niederlande – Bündnis für humane Bildung – Deutschland – Center for Civil and Human Rights (Poradňa) – Slowakei – Center for Democracy & Technology – Europa – Chaos Computer Club – Deutschland – Centrum Cyfrowe – Europa – Bürger D / Državljan D – Slowenien – Civil Liberties Union for Europe – Europa – CloudPirat – Deutschland – Committee to Protect Journalists – EU/International – comun.al – Lateinamerika – COMMUNIA Association for the Public Domain – Europa – D64 – Zentrum für Digitalen Fortschritt – Deutschland – Dataskydd.net – Schweden – Defend Democracy – International – Defend Digital Me – Vereinigtes Königreich – Democracy in Europe Movement 2025 (DiEM25) – Europa – **Deutsche Vereinigung für Datenschutz e.V. (DVD) – Deutschland** – DFRI – Schweden – Digital Advisor – Niederlande – Digitalcourage – Deutschland – Digitale Gesellschaft – Deutschland – Digitale Gesellschaft / Digital Society – Schweiz – Digitale Rechte Irland – Irland – Europäische Digitale Rechte (EDRi) – Europa – European Sex Workers' Rights Alliance (ESWA) – Europa und Zentralasien – Electronic Frontier Finland – Finnland – Elektronisk Forpost Norge (EFN) – Norwegen – Electronic Frontier Foundation (EFF) – Vereinigte Staaten – Electronic Privacy Information Center (EPIC) – International – epicenter.works for digital rights – Österreich – Equipo Decenio Afrodescendiente – Spanien – Eticas Foundation – International – Europäisches Zentrum für Non-Profit-Recht (ECNL) – Europa – Europäische Journalistenvereinigung (EJF) – Europa – Fight for the Future – US/International – Fitug e.V. – Deutschland – Fundación Karisma – Kolumbien – The Foundation for Information Policy Research (FIPR) – Großbritannien/Europa – Global Forum for Media Development – International – GAT – Grupo de Ativistas em Tratamentos – Portugal – Gesellschaft für Bildung und Wissen e.V. – Deutschland – Hermes Center for Transparency and Digital Human Rights – Italien – Homo Digitalis – Griechenland – Human Rights House Zagreb – Kroatien – imaniti.org – Tschechische Republik – iNGO European Media Platform – Europa – International Press Institute (IPI) – International – Internet Governance Project – International – Internet Society – International – Interpeer gUG (gemeinnützig) – Europa – Irischer Rat für bürgerliche Freiheiten – Irland – ISOC Brazil – Brazilian Chapter of the Internet Society – Brasilien – Internet Society Catalan Chapter (ISOC-CAT) – Europa – ISOC UK England – Großbritannien – IT-Pol – Dänemark – Iuridicum Remedium, z.s – Tschechische Republik – La Quadrature du Net – Frankreich – Ligue des droits humains – Belgien – LOAD e.V. – Deutschland – Lobby4kids – Kinderlobby- Österreich – Medienkompetenz Team e.V. – Deutsch-

land – Netherlands Helsinki Committee – Niederlande – Nordic Privacy Center – Nordische Länder – Norwegen Chapter der Internet Society – Norwegen – Norwegische Unix-Benutzergruppe – Norwegen – Österreichischer Rechtsanwaltskammertag – Österreich – Open Rights Group – Vereinigtes Königreich – quintessenz – Verein zur Wiederherstellung der Bürgerrechte im Informationszeitalter – Österreich – Panoptykon Foundation – Polen – Peace Institute – Slowenien – PIC Amsterdam – Niederlande – Plattform Bürgerrechte – Niederlande – Presseclub Concordia – Österreich – Privacy First – Niederlande – Privacy International – International – Ranking Digital Rights – International – Red Umbrella – Schweden – SaveThe-Internet – Europa – SekswerkExpertise – Niederlande – Sex Workers Alliance Irland – Irland – Sex Workers' Empowerment Network – Griechenland – SMEX – MENA – Social Media Exchange – Naher Osten und Nordafrika (MENA) – SZEXE – Verband der ungarischen Sexarbeiterinnen – Ungarn – StatewatchEU – Europa – Stowarzyszenie Nasze Imaginarium – Polen – Teckids e.V. – Deutschland – S.T.O.P. – The Surveillance Technology Oversight Project – Vereinigte Staaten – Stichting Stop Online Shaming – Niederlande – Voices4 Berlin – International – Vrijschrift.org – Niederlande – Whistleblower-Netzwerk – Deutschland – Whose Knowledge? – International – Wikimedia – International – Wikimedia Deutschland e.V. – Deutschland – Women's Link Worldwide – Europa – WorkerInfoExchange – International – Xnet – Spanien.

Der englischsprachige Originaltext findet sich unter:
https://chat-kontrolle.eu/wp-content/uploads/2022/06/Offener-Brief-EDRi-CSA-englisch.pdf

Presseerklärung vom 10.10.2022

Zivilgesellschaft gegen EU-Pläne zur Chatkontrolle

Neben der Deutschen Vereinigung für Datenschutz richten sich aktuell 22 zivilgesellschaftliche Organisationen in einem öffentlichen Aufruf gegen die Pläne der Europäischen Kommission zur massenhaften Überwachung von Kommunikation und Onlineinhalten.

Die Pläne würden massiv in die Grundrechte der gesamten europäischen Bevölkerung eingreifen und eine dystopische Überwachungsinfrastruktur etablieren. Statt tatsächlich den Schutz von Kindern, also Prävention und Opferschutz, in den Mittelpunkt ihrer Maßnahmen zu stellen, setzt die Kommission auf eine vermeintliche „technische" Lösung, die Überwachung in demokratiegefährdendem Umfang ermöglicht.

Die Kampagne „Chatkontrolle stoppen" wendet sich entschieden dagegen und fordert von den politisch dafür Verantwortlichen von diesen Plänen Abstand zu nehmen.

Tom Jennissen, von der Digitalen Gesellschaft e.V.: „Wir fordern die gesamte Bundesregierung und insbesondere das verhandlungsführende Bundesinnenministerium auf entschieden gegen die dystopischen Pläne zur Chatkontrolle einzutreten. Sie muss endlich ihren Einfluss im Europäischen Rat geltend machen, um die Verordnung zu verhindern."

Julia Witte, von Digitalcourage e.V.: „Die Überwachungsinfrastruktur, die nötig wäre, um den Vorschlag der Kommission umzusetzen, widerspricht den grundlegenden Werten unserer Gesellschaft. Wenn keine unbeobachtete Kommunikation mehr möglich ist, ist das eine Katastrophe."

Frank Spaeing, von der Deutschen Vereinigung für Datenschutz e.V. (DVD): „Das Bundesinnenministerium muss sich – nachdem selbst Kinderschutzorganisationen die Sinnhaftigkeit der EU-Pläne zur Chatkontrolle verneint haben (und um den Schutz der Kinder geht es bei diesen Maßnahmen ja scheinbar) – auf die eigenen Aussagen im Koalitionsvertrag besinnen, nach denen die Koalitionäre Maßnahmen zum Scannen privater Kommunikation und eine Identifizierungspflicht ablehnen, und sich aktiv dafür einsetzen diese Verordnung zu verhindern."

Zum Hintergrund:

Im Mai hat die EU-Kommission einen Verordnungsentwurf zur Bekämpfung von Kindesmissbrauch vorgelegt. Der Vorschlag sieht unter anderem vor Kommunikations- und Hostingdiensteanbietern dazu zu verpflichten sämtliche Inhalte aller Nutzenden nach verdächtigem Material zu durchleuchten und Verdachtsfälle an eine zentrale Stelle weiterzuleiten. Das würde bedeuten, dass beispielsweise Messengerdienste wie WhatsApp oder Signal private Chats aller Nutzer:innen durchsuchen müssten. Auch Maßnahmen wie verpflichtende Alterskontrollen oder Netzsperren werden vorgeschlagen.

Ende-zu-Ende-verschlüsselte Kommunikation ist im Verordnungsvorschlag ausdrücklich nicht ausgenommen. Das Durchleuchten verschlüsselter Kommunikation ist aber technisch nur möglich, wenn die Verschlüsselung insgesamt gebrochen oder untergraben wird – etwa indem das eigene Gerät mittels Technologien wie Client-Side-Scanning zur Überwachung genutzt wird.

Da sämtliche elektronische Kommunikation – von Messengerdiensten über E-Mail bis zur Sprachtelefonie (betreffend „Grooming") – sowie Hosting betroffen sein kann, würde dies zu einem faktischen Ende des elektronischen Brief- und Fernmeldegeheimnisses führen. Umsetzbar wäre dies nur durch den

Aufbau einer umfassenden technischen Infrastruktur, die nicht nur fehler- und missbrauchsanfällig ist, sondern auch jederzeit um weitere Deliktsfelder erweitert werden kann.

Liste der Erstunterzeichner: Algorithmwatch, ArGE Tübingen, Berliner Wassertisch, ChaosComputerClub, D64 e.V., Dachverband der Fanhilfen e.V., Digitalcourage, Digitale Freiheit, Digitale Gesellschaft, **Deutsche Vereinigung für Datenschutz e.V. (DVD)**, FifF – Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, Gesellschaft für Informatik, Giordano-Bruno-Stiftung, Humanistische Union, Humanistische Union Berlin-Brandenburg, Komitee für Grundrechte und Demokratie, Load e.V., MOGiS e. V. - Eine Stimme für Betroffene, RAV – Republikanischer Anwält*innen- und Anwälteverein e.V., Reporter ohne Grenzen, Superrr Lab, Whistleblower Netzwerk, Zwiebelfreunde e.V.

Nobelpreisträger starten Aufruf zur Bekämpfung der „existenziellen Bedrohung“ für die Demokratie durch das Geschäftsmodell von Big Tech

Die Friedensnobelpreisträger Maria Ressa und Dmitry Muratov haben am 2. September 2022 zusammen mit anderen Unterzeichnenden einen Aufruf gestartet, um die schädlichen Auswirkungen des Geschäftsmodells von Big Tech zu bekämpfen und deren bewusste Verstärkung von Desinformation, Hassreden und Internetmissbrauch zu beenden.

Maria Ressa: „Das enorme Potenzial der Technologie zur Weiterentwicklung unserer Gesellschaften wurde von Big Tech mit einem Geschäftsmodell gekapert, das vorsätzlich Lügen und Desinformation im Namen des Profits fördert.“

Dmitry Muratov: „Die Unterstützung und Investition in wirklich unabhängige Medien ist ein Gegenmittel gegen die Verzerrung von Fakten und die Polarisierung der Debatte in der Gesellschaft.“

Ein 10-Punkte-Plan zur Bewältigung unserer Informationskrise

Wir appellieren an alle rechtsstaatlichen demokratischen Regierungen:

1. Verlangen Sie von Technologieunternehmen, dass diese unabhängige Folgenabschätzungen zu Menschenrechten durchführen, die veröffentlicht werden müssen, und fordern Sie Transparenz in allen Aspekten ihres Geschäfts – von der Moderation von Inhalten über die Auswirkungen von Algorithmen bis hin zur Datenverarbeitung und zu Integritätsrichtlinien.
2. Schützen Sie das Recht der Bürger auf Privatsphäre mit wirkungsvollen Datenschutzgesetzen.
3. Verurteilen Sie öffentlich die Angriffe auf die freie Presse und Journalisten weltweit und unterstützen und finanzieren Sie angegriffene unabhängige Medien und Journalisten.

Wir appellieren an die EU:

4. Bringen Sie zügig die Durchsetzung des Digital Services Act und des Digital Markets Acts voran, damit diese Gesetze für die Unternehmen nicht nur „neuer Papierkram“ sind und diese vielmehr gezwungen werden ihr Geschäftsmodell zu ändern, z. B. dass diese die automatisierte Auswertung beenden, mit der Grundrechte bedroht und Desinformation und Hass verbreitet werden, auch wenn diese Risiken ihren Ursprung außerhalb der EU haben.
5. Bringen Sie unbedingt Gesetze zum Verbot von Überwachungswerbung voran, da diese Praxis grundsätzlich nicht mit den Menschenrechten vereinbar ist.
6. Setzen Sie die EU-Datenschutz-Grundverordnung wirksam um, damit die Datenrechte der Menschen endlich Wirklichkeit werden.
7. Sehen Sie starke Schutzvorkehrungen für die Sicherheit von Journalisten, die Nachhaltigkeit der Medien und demokratische Garantien im digitalen Raum im Rahmen des geplanten Europäischen Gesetzes zur Medienfreiheit vor.
8. Schützen Sie die Medienfreiheit, indem Sie Desinformation im Internet unterbinden. Das bedeutet, dass es keine besonderen Ausnahmen oder Privilegierungen für Organisationen oder Einzelpersonen in Gesetzen zu neuen Technologien oder Medien geben sollte. Bei globalisierten Informationsflüssen würde dies jenen Regierungen und nichtstaatlichen Akteuren einen Blankoscheck ausstellen, die Desinformationen im industriellen Maßstab produzieren, um Demokratien zu schaden und um überall Gesellschaften zu polarisieren.
9. Stellen Sie sich der außergewöhnlichen Lobby-Maschinerie entgegen, mit deren Astroturfing-Kampagnen und den Personalkaruselle zwischen den großen Technologieunternehmen und europäischen Regierungsinstitutionen (Astroturfing bezeichnet politische oder kommerzielle Werbeprojekte, die eine spontane Aktivitäten von unten vortäuschen).

Wir appellieren an die Vereinten Nationen (UN):

10. Schaffen Sie einen Sondergesandten des UN-Generalsekretärs mit der Aufgabe die Sicherheit von Journalisten (SESJ) zu erhöhen, der deren aktuelle Bedrohung angeht und endlich die Kosten für Verbrechen gegen Journalisten erhöht.

Unterzeichnet durch die Nobelpreisträger des Jahres 2021
Dmitry Muratov und Maria Ressa

Unterstützer:
Amnesty International, Nobelpreisträger 1977; Beatrice Fihn, Executive Director, ICAN – the International Campaign to Abolish Nuclear Weapons, Nobelpreisträgerin 2017; Kailash Satyarthi, Nobelpreisträger 2014: Jody Williams, Nobelpreisträgerin 1997; Juan Manuel Santos, Nobelpreisträger 2016; Leymah Gbowee, Nobelpreisträgerin 2011; Nadia Murad, Nobelpreisträgerin 2018; Shirin Ebadi, Nobelpreisträgerin 2003; Tawakkol Karman, Nobelpreisträger 2011; Alexandra Geese, Mitglied des Europaparlaments; Bruce Mutsvairo, Professor, Media and Performance Studies, University of Utrecht; Can Dundar, türkischer Exiljournalist; Carole Cadwaladr, Journalistin von Guardian & Observer & Mitgründerin The Real Facebook Oversight Board; Christophe Deloire, Vorstand Forum on Information and Democracy; David Carroll, Professor für Mediendesign, The New School; Frances Haugen, Facebook Whistleblowerin; Gerard Ryle, Direktor International Consortium of Investigative Journalists; Irene Khan, Berichterstatterin für Meinungsfreiheit im Amt des UN-Hohen Kommissars für Menschenrechte; Julie Posetti, stellvertretende Präsidentin Forschungsdirektorin, International Center for Journalists; Khadija Patel, Vorstand International Press Institute; Marietje Schaake, Stanford Cyber Policy Center; Mogens Blicher Bjerregård, internationaler Berater Danish Union of Journalists; Peter Pomerantsev, Senior Fellow Johns Hopkins University; Paul Tang, Mitglied des Europaparlaments; Phumzile van Damme, Tech.Activistin und frühere Abgeordente in Südafrika; Roger McNamee, ehemaliger Berater von Facebook-CEO Mark Zuckerberg, Autor von „Zucked: Waking Up to the Facebook Catastrophe“; Safiya Umoja Noble, Professorin und Autorin von „Algorithms of Oppression: How Search Engines Reinforce Racism“; Shoshana Zuboff, Autorin von „The Age of Surveillance Capitalism“, emeritierte Professorin Harvard Business School, Beirat International Observatory on Information and Democracy; Staffan I. Lindberg, Professor Politikwissenschaft, Universität Gothenburg; Susie Alegre, Menschenrechtsanwälting und Autorin von „Freedom to Think: The Long Struggle to Liberate Our Minds“

sowie

Access Now, Alliance4Europe, All Out Action Fund, ASEAN Parliamentarians for Human Rights, Avaaz, Burmese Rohingya Organisation UK, Center for Democracy and Technology, Centre for Research on Multinational Corporations, Centre for Peace Studies, Corporate Europe Observatory, Digitalcourage e.V., Digital Society Switzerland, Defend Democracy, Demos, **Deutsche Vereinigung für Datenschutz e.V. (DVD)**, digiQ, Digital Content Next, D64 - Zentrum für Digitalen Fortschritt, Electronic Frontier Finland (Effi), Elektronisk Forpost Norge, Estonian Human Rights Centre, European Digital Rights (EDRi), EU DisinfoLab, European Federation of Public Service Unions, Freedom United, Free Expression Myanmar, Freemuse, Free Press (United States), Foxglove, Global Project Against Hate and Extremism, Global Witness, Human Rights Watch, Hacked Off, HateAid, I Am Here International, Irish Council of Civil Liberties, KaskoSan Roma Charity, Kofi Annan Foundation, Larger Us, Lie Detectors, Luminate, Missing Children Europe, Movement Against Disinformation Philippines, Nadia's Initiative, National Center on Race and Digital Justice (U.S.), Open Rights Group, Panoptykon Foundation, People vs. Big Tech, Progressive Voice Myanmar, Transparency International EU, UCLA Center for Critical Internet Inquiry, Victims Advocate International, Waag, WeMove Europe, Wikimedia Deutschland, 5 Rights Foundation, #jesuislà, #ShePersisted.

Der englischsprachige Text des Aufrufs ist u.a. veröffentlicht unter https://peoplevsbig.tech/10-point-plan

Offener NGO-Brief an SPD, Grüne und FDP vom 19. September 2022

Keine anlasslose Vorratsdatenspeicherung von IP-Adressen!


Bild: iStock.com / kynny

Sehr geehrte Frau Nancy Faeser, Bundesministerin des Innern und für Heimat,
sehr geehrter Herr Marco Buschmann, Bundesminister der Justiz,
sehr geehrte Frau Lisa Paus, Bundesministerin für Familie, Senioren, Frauen und Jugend,
sehr geehrter Herr Lars Klingbeil, Bundesvorsitzender der SPD,
sehr geehrter Herr Omid Nouripour,

Bundesvorsitzender von BÜNDNIS 90/DIE GRÜNEN,
sehr geehrte Frau Ricarda Lang, Bundesvorsitzende von BÜNDNIS 90/DIE GRÜNEN und
sehr geehrter Herr Christian Lindner, Bundesvorsitzender der FDP

Die unterzeichnenden Organisationen und Personen dieses Briefs lehnen die anlasslose Vorratsdatenspeicherung der IP-Adressen aller Bürger:innen ab und fordern Sie auf den Koalitionsvertrag umzusetzen, die Freiheitsrechte der Bevölkerung zu schützen und langfristig den Weg einer massenüberwachungsfreien Politik einzuschlagen. Stoppen Sie die Vorratsdatenspeicherung, schützen Sie Telefon- und auch Internetnutzer:innen!

Privatsphäre ist Grundrecht. Keine anlasslose Vorratsdatenspeicherung von IP-Adressen!

Die aktuellen Regelungen zur Vorratsdatenspeicherung, deren Anwendung seit Juli 2017 nach einem Beschluss des Oberverwaltungsgerichts Nordrhein-Westfalen ausgesetzt sind, verpflichten öffentlich zugängliche Internetzugangsdienste zur pauschalen Speicherung aller IP-Adressen, die den Endnutzer:innen für eine Internetnutzung zugewiesen wurden, inklusive einer eindeutigen Kennung des Anschlusses, einer zugewiesenen Benutzerkennung sowie Datum und Uhrzeit von Beginn und Ende der Internetnutzung. Im Falle von Internet-Sprachkommunikationsdiensten müssten auch die IP-Adressen des anrufenden und des angerufenen Anschlusses und die zugewiesene Benutzerkennungen gespeichert werden.

Am 20. September wird der Gerichtshof der Europäischen Union seine Entscheidung über das deutsche Gesetz zur Vorratsdatenspeicherung verkünden. In den darauf folgenden Monaten geht es um die Erfüllung des Koalitionsvertrags [1]. Die Bundesregierung will sich laut Vertrag von der Überwachungspolitik der Vorgängerregierung konsequent abwenden und die „Regelungen zur Vorratsdatenspeicherung so ausgestalten, dass Daten rechtssicher anassbezogen und durch richterlichen Beschluss gespeichert werden können."

Koalitionsvertrag einhalten!

Der Koalitionsvertrag schließt jede Form der anlasslosen Speicherung der Kommunikationsdaten der Bürgerinnen und Bürger aus. Das betrifft auch die von der Bundesinnenministerin erhobene Forderung [2] nach der Einführung einer anlasslosen und pauschalen IP-Vorratsdatenspeicherung. Wir rufen Sie auf die Versprechen des Koalitionsvertrags gegenüber den Bürgerinnen und Bürgern einzuhalten!

Schwerer Eingriff in die Grundrechte: IP-Daten bedingen Verfolgung und Profilbildung von Menschen

Regierungen, Parlamente und große Teile der Bevölkerung unterschätzen das Risiko von IP-Adressen für das tägliche Leben. In seinem Urteil aus Oktober 2020 (La Quadrature du Net) betont der EU-Gerichtshof die Sensibilität von IP-Daten: „Da die IP-Adressen jedoch insbesondere zur umfassenden Nachverfolgung der von einem Internetnutzer besuchten Internetseiten und infolgedessen seiner Online-Aktivität genutzt werden können, ermöglichen sie die Erstellung eines detaillierten Profils dieses Nutzers. Die für eine solche Nachverfolgung erforderliche Vorratsspeicherung und Analyse der IP-Adressen stellen daher schwere Eingriffe in die Grundrechte des Internetnutzers aus den Art. 7 und 8 der Charta dar und können abschreckende Wirkungen wie die in Rn. 118 des vorliegenden Urteils dargelegten entfalten."

Zuletzt bestätigte eine Studie[3] zu Privatsphäre und IPv6-Adressen, dass IP-Adressen trotz Vorkehrungen zum Datenschutz eindeutige und dauerhafte Tracking-Identifikatoren sein können.

IP-Vorratsdatenspeicherung ist ungeeignet für den Schutz von Kindern

In Deutschland werden Forderungen nach massenhafter Speicherung von Kommunikationsdaten hauptsächlich mit dem Schutz von Kindern und Jugendlichen vor sexualisierter Gewalt begründet. Im November 2021 hatte der Arbeitskreis gegen Vorratsdatenspeicherung gemeinsam mit zehn weiteren Bürgerrechts- und Berufsverbänden dargelegt, warum Vorratsdatenspeicherung zum Schutz von Kindern ungeeignet [4] ist. Im Januar 2022 bestätigte eine Antwort der Bundesregierung auf eine schriftliche Frage zudem, dass Vorratsdatenspeicherung nicht notwendig ist. Laut Daten des Bundeskriminalamts [5] konnten nur 3 % alle Fälle der „Nutzung, des Handels oder der Verbreitung von Kinderpornographie in den Jahren 2017 bis 2021" aufgrund nicht vorhandener IP-Adressen nicht weiter verfolgt werden.

Im April 2022 kritisierte gegen-missbrauch e.V. [6]: „(...) das Problem ist nicht die [fehlende Vorratsdatenspeicherung], sondern, das[s] die Ermittlungsbehörden vom Personal und der Ausstattung noch im 19. Jahrhundert sind, und Täter:innen tatsächlich im Jahr 2022".

Vorratsdatenspeicherung hilft nicht für mehr Sicherheit

Der Arbeitskreis gegen Vorratsdatenspeicherung (AKV) betont in seiner Analyse [7] einer Studie [8] des Max-Planck-Instituts aus 2011:

„Dass Straftäter heutzutage oftmals elektronisch statt wie früher mündlich oder postalisch kommunizieren, bedeutet also nicht, dass die Benutzung der Kommunikationsnetze total nachvollziehbar sein müsste, wie es auch bei der mündlichen und postalischen Kommunikation nie der Fall gewesen ist." Der AKV hebt hervor: „Im Jahr 2020 wurde die Verbreitung pornografischer Schriften laut Kriminalstatistik zu 91,3% aufgeklärt - ohne dass eine Pflicht zur IP-Vorratsdatenspeicherung in Kraft ist!"

Die Studie kommt daher zu dem Ergebnis: „Insbesondere gibt es bislang keinen Hinweis dafür, dass durch eine umfängliche Verfolgung aller Spuren, die auf das Herunterladen von Kinderpornografie hindeuten, sexueller Missbrauch über den Zufall hinaus verhindert werden kann." (221f)

Umgekehrt gilt, dass anonyme Kommunikation Kinder schützt, indem sie anonyme Beratung, Selbsthilfe und Strafanzeigen ermöglicht.

Anstelle von Massenüberwachung sind es gezielte und unmittelbare Maßnahmen, die Kinder und Jugendliche schützen können. Dazu gehören bes-

sere und schnellere gezielte Ermittlungen, Schutz- & Präventionskonzepte an Schulen und kirchlichen Einrichtungen sowie die Stärkung der Kompetenzen von Kontaktpersonen in Behörden, Beratungsstellen und öffentlichen Einrichtungen.

Vorratsdatenspeicherung trifft unschuldige Bürger:innen

Während sich Kriminelle technisch vor Massenüberwachung schützen können, würde eine pauschale Vorratsdatenspeicherung vor allem rechtstreu lebenden Menschen erfassen und schwer in ihren Grundrechten verletzen. Überwachung muss in einer Demokratie die Ausnahme bleiben und darf niemals zum Standard werden.

Recht auf vertrauliche Internetnutzung

Die vertrauliche und anonyme Internetnutzung ist für die Meinungs- und Informationsfreiheit unerlässlich. Eine generelle und verdachtslose Vorratsspeicherung unserer Identität und IP im Internet würde das Ende der Anonymität im Internet bedeuten. Sie würde es den meisten Bürger:innen unmöglich machen das Internet frei vom Risiko staatlicher Beobachtung (z.B. auch wegen eines falschen Verdachts), missbräuchlicher Offenlegung durch Mitarbeiter:innen des Anbieters und versehentlichen Datenverlustes zu nutzen. Dadurch hätte eine IP-Vorratsdatenspeicherung unzumutbare Folgen, wo Menschen nur im Schutz der Anonymität überhaupt bereit sind sich in einer Notsituation beraten und helfen zu lassen (z.B. Opfer und Täter:innen von Gewalt- oder Sexualdelikten), ihre Meinung trotz öffentlichen Drucks zu äußern oder Missstände bekannt zu machen (Presseinformanten, anonyme Strafanzeigen, ausländischeDissidenten). Bürger:innen müssen die Möglichkeit haben sich anonym mit Journalist:inn:en, Behörden, Anwaltskanzleien, Beratungsstellen und Ärzt:inn:en auszutauschen ohne dabei rückverfolgt werden zu können.

Massenüberwachungsfreie Politik

Wir fordern Sie auf den Koalitionsvertrag umzusetzen, die Freiheitsrechte der Bevölkerung zu schützen und langfristig den Weg einer massenüberwachungsfreien Politik einzuschlagen.

Stoppen Sie die Vorratsdatenspeicherung, schützen Sie Telefon- und auch Internetnutzer:innen!

Erstunterzeichnende Organisationen und Personen

- Aktion Freiheit statt Angst e.V.
- AlgorithmWatch
- Deutsche Aidshilfe
- **Deutsche Vereinigung für Datenschutz e.V. (DVD)**
- DFJV Deutscher Fachjournalisten-Verband AG
- DieDatenschützerRhein-Main
- Digitalcourage e.V.
- Digitale Gesellschaft e. V.
- Dr. Rolf Gössner, Jurist/Publizist, Kuratoriumsmitglied der Internationalen Liga für Menschenrechte
- Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V.
- freiheitsfoo / freiheitsfoo.de
- Humanistische Union e.V.
- Komitee für Grundrechte und Demokratie e.V.
- mailbox.org – Heinlein Hosting GmbH
- Monique Hofmann – Bundesgeschäftsführerin Deutsche Journalistinnen- und Journalisten-Union (dju) in ver.di
- Netzwerk Recherche
- Neue Richtervereinigung e.V., Bundesvorstand
- openPetition
- Peter Leppelt – Mitglied des Digitalrat Niedersachsen
- Prof. Dr. Clemens Arzt – FÖPS Berlin – Forschungsinstitut für öffentliche und private Sicherheit (Gründungsdirektor)
- Prof. Dr. Fredrik Roggan – Hochschule der Polizei des Landes Brandenburg
- Prof. Dr. Ira Diethelm – Carl von Ossietzky Universität
- Prof. Dr.-Ing. Tibor Jager – Bergische Universität Wuppertal
- Prof. Thorsten Holz – CISPA Helmholtz Center for Information Security
- Reporter ohne Grenzen e. V. / Reporters Without Borders (RSF) Germany
- Republikanischer Anwältinnen- und Anwälteverein e.V. (RAV)



Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

PNR-Datenerfassung und -auswertung muss eingeschränkt werden

Das Bundeskriminalamt (BKA) muss die anlasslose Fluggastüberwachung nach dem Urteil des Europäischen Gerichtshofs (EuGH) vom 21.06.2022 (Az. C-817/19, DANA 3/2022, 201 ff.) massiv einschränken. Das BKA hat gemäß einer Antwort an die Presse seit dem Start der Flugverkehrsüberwachung im August 2018 bis April 2022 die Datensätze von 145.821.880 Fluggästen gespeichert und ausgewertet. Erfasst werden rund 40 Millionen Flugreisen pro Jahr. Geregelt ist das im Fluggastdatengesetz, das 2017 in Kraft trat und die PNR-Richtlinie der EU (2016/681) zu Passenger Name Records (PNR) umsetzt. Erfasst werden dabei alle Flüge in die EU hinein und heraus sowie alle Flüge zwischen den EU-Staaten. Nur bei rein innerstaatlichen Reisen (beispielsweise von München nach Hamburg) werden die Passagierdaten nicht gespeichert.

Die Fluggastdaten werden mit polizeilichen Datenbanken abgeglichen, um zum Beispiel flüchtige Straftäter zu erwischen. Laut BKA gab es seit dem Start 20.012 Fahndungserfolge beim Register-Abgleich. Zudem sollen bisher unbekannte Straftäter anhand bestimmter „Muster" erkannt werden. Wer zum Beispiel die gleichen Reiserouten nutzt wie Drogenkuriere und sich auch sonst wie ein Drogenkurier verhält, muss mit einer individuellen Überprüfung rechnen. Das BKA meldet beim Muster-Abgleich 670 Treffer in knapp vier Jahren. Das BKA, das in Deutschland für die Speicherung und Auswertung der Flugdaten zuständig ist, bewertet die Fluggastdatenauswertung als „effektives System". Auch eine Ausweitung der Überwachung auf den grenzüberschreitenden Flug- und Fährverkehr hält das BKA für „sinnvoll". Politisch ist das derzeit nicht geplant.

Der EuGH hat im Juni 2022 auf Vorlage des belgischen Verfassungsgerichts zur PNR-Richtlinie der EU entschieden, dass diese nur dann mit EU-Recht vereinbar ist, wenn sie „eng ausgelegt" und die Befugnisse der Behörden auf das „absolut Notwendige" begrenzt werden. Der EuGH verlangt, dass die Fluggastdaten nicht mehr fünf Jahre lang gespeichert werden, sondern grundsätzlich nur noch sechs Monate. Zwar wurden die Daten bisher schon nach sechs Monaten „depersonalisiert", die Namen der Fluggäste waren in der Datei also nicht mehr zu sehen. Doch auf richterlichen Beschluss konnte die Depersonalisierung rückgängig gemacht werden. Laut BKA ist dies in 670 Fällen auch erfolgt. Künftig ist das nicht mehr möglich, weil die Fluggastdaten nach sechs Monaten völlig gelöscht werden müssen.

Der EuGH hat auch die Gründe der Auswertung reduziert. Sie muss sich künftig auf die Verhinderung und Aufklärung von terroristischen Straftaten und von Taten, die mit dem Flugverkehr zu tun haben, etwa Flugzeugentführungen, beschränken. Datenabgleiche wegen anderer Delikte wie Mord, Vergewaltigung und Umweltkriminalität sind künftig rechtlich nicht mehr möglich. Nur 5% der bisherigen Treffer hatten laut BKA mit Terror zu tun. Über den Anteil der Treffer bei flugbezogenen Taten lagen keine Zahlen vor. Zudem hat der EuGH eine anlasslose Speicherung und Auswertung der Fluggastdaten bei Flügen innerhalb der EU vor allem darauf beschränkt, dass eine akute terroristische Bedrohung vorliegen muss. Laut BKA betreffen bisher aber immerhin 61% der Datensätze „Intra-EU-Flüge". Der Großteil der Speicherung muss also entfallen.

Für das größte Aufsehen sorgte der EuGH mit der Auflage, dass bei der Erkennung verdächtiger Muster keine maschinell lernenden Systeme und keine unkontrollierte künstliche Intelligenz mehr eingesetzt werden darf. Der EuGH sah darin die Gefahr, dass die so entstehenden Algorithmen zu Falschverdächtigungen führen. In den Jahren 2018 und 2019 seien in manchen Staaten immerhin fünf von sechs Treffern „falsch positiv" gewesen, führten also zu einem falschen Verdacht. Insofern haben die EuGH-Vorgaben nur geringe Auswirkungen auf Deutschland. Das BKA versicherte, dass es bei der Mustererkennung keine künstliche Intelligenz und keine maschinell lernenden Systeme einsetzt. Zwar arbeitet auch das BKA mit vermeintlich verdächtigen Reisemustern, die aber auf dem Erfahrungswissen von Kriminalpolizisten beruhen.

Das BKA ist gemäß einer Sprecherin mit den bevorstehenden Einschränkungen unzufrieden. Sie seien „nicht förderlich" für eine effektive Strafverfolgung und die Gewährleistung von Sicherheit. Wann das deutsche Fluggastdatengesetz entsprechend geändert wird, ist noch nicht absehbar. Das von Nancy Faeser (SPD) geleitete Bundesinnenministerium wertet die EuGH-Entscheidung noch aus: „Bereits jetzt ist aber absehbar, dass sie zu deutlichen Einschränkungen für die Verarbeitung von Fluggastdaten führt." Nach Abschluss der Auswertung werde das Ministerium die erforderlichen Anpassungen des Fluggastdatengesetzes „anstoßen".

Beim EuGH liegen auch fünf Vorlagen aus Deutschland, zwei vom Verwaltungsgericht (VG) Wiesbaden, drei vom Amtsgericht (AG) Köln; alle Klagen wurden von der GFF (Gesellschaft für Freiheitsrechte) koordiniert. Nach den nun vorliegenden Vorgaben des EuGH dürften sich die Vorlagen erledigt haben, so dass die Gerichte voraussichtlich zeitnah entscheiden werden. Das AG Köln muss klären, ob Fluggesellschaften Daten ihrer Fluggäste an das BKA weitergeben dürfen. Beim VG Wiesbaden geht es um die Frage, ob das BKA diese Daten

speichern und auswerten darf (Rath, Weniger Rasterfahndung am Himmel, https://taz.de/Speicherung-von-Fluggastdaten/!5875810/ 22.08.2022).

Bund

Kritisiertes Forschungsdatenzentrum geht in Betrieb

Von August 2022 bis spätestens zum 1. Oktober mussten die Krankenkassen im Rahmen des sog. Datentransparenzverfahrens besonders schützenswerte Gesundheitsdaten ihrer 73 Millionen gesetzlich Versicherten zu Forschungszwecken bereitstellen. Sie sollten zwischen dem ersten August und dem ersten Oktober 2022 an die Sammelstelle des Spitzenverbands Bund der Krankenkassen (GKV-Spitzenverband) übermittelt werden. Inzwischen sind alle Abrechnungsdaten der Versicherten dort eingetroffen. Bis zum ersten Dezember 2022 werden die Daten dann an das am Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) eingerichtete Forschungsdatenzentrum (FDZ) weitergeleitet werden. Anschließend soll die Datensammlung immer weiter ergänzt und bis zu 30 Jahre lang gespeichert werden. Ein Widerspruchsrecht und auch sonstige Betroffenenrechte sind nicht vorgesehen. Die Gesellschaft für Freiheitsrechte (GFF) kritisiert das und will weiter gegen mangelnden Datenschutz vorgehen. Sie sieht darin einen Verstoß gegen das Recht auf informationelle Selbstbestimmung und z.B. gegen Artikel 21 der DSGVO.

Die GFF hat Anfang Mai 2022 gemeinsam mit Constanze Kurz vom Chaos Computer Club (CCC) und einer Person, die an dem seltenen Krankheitsbild Hämophilie leidet, zwei Eilverfahren bei den Sozialgerichten in Berlin und Frankfurt eingeleitet, um die Weitergabe der Daten zunächst in zwei Fällen zu verhindern. Die GFF hält die Nutzung von Gesundheitsdaten für Forschungszwecke für sinnvoll, doch würden die „bislang gesetzlich vorgesehenen Schutzstandards" für die Gesundheitsdatenbank nicht ausreichen. Die Daten würden lediglich pseudonymisiert, wobei Angaben wie Name und Geburtstag entfernt werden. Ein Gutachten des Kryptografie-Professors Dominique Schröder hatte jedoch gezeigt, dass trotzdem Rückschlüsse auf einzelne Personen möglich sind. Ein Missbrauch der Daten könne nicht ausgeschlossen werden, u.a. wegen des Fehlens einer Pflicht zum Einsatz zeitgemäßer Verschlüsselung.

Vor allem die zentrale Datensammlung beim GKV-Spitzenverband und in dem FDZ sieht Schröder kritisch; sie sei ein möglicher Single Point of Failure und nicht notwendig. Besser sei eine dezentrale Datenspeicherung, die auch dem Stand der Technik entspricht. Auch die Gematik arbeitet derzeit an einem Konzept, bei dem Daten nicht zentral gespeichert werden. Als Methoden für den Umgang mit sensiblen Daten nennt Schröder unter anderem das Konzept „Differential Privacy", das auch von Google und Apple eingesetzt wird. Auch schlägt er den Einsatz moderner kryptografischer Verfahren wie die Verwendung homomorpher Verschlüsselungen oder die der sicheren Mehrparteienberechnung vor.

Die GFF will mit weiteren Klagen ein Widerspruchsrecht erwirken und „dass die Daten der Versicherten bestmöglich geschützt werden, um einen Missbrauch zu verhindern". Dabei sollten bei der „Zusammenführung der Datensätze vor der Pseudonymisierung, der zentralen Speicherung der pseudonymisierten Datensätze sowie der Verarbeitung der Daten durch die Nutzungsberechtigten hohe IT-Sicherheitsstandards" gelten. Bijan Moini, Jurist und Verfahrenskoordinator von GFF, erläuterte: „Wer an einer seltenen Krankheit leidet, ist in scheinbar anonymisierten Datenbanken besonders leicht identifizierbar. Das ist besonders dann gefährlich, wenn die Krankheit stigmatisierend wirkt oder die Kenntnis davon sogar Erpressungspotenzial hat." Niemand wolle Gesundheitsforschung verhindern, „aber das Gesetz sieht weder ausreichende Schutzstandards noch moderne Verschlüsselungsmethoden vor – das ist fahrlässig und gefährlich. Wenn Gesundheitsdaten einmal in falsche Hände geraten, kann das nicht mehr rückgängig gemacht werden!"

Das Bundesgesundheitsministerium wollte sich zu dem „laufenden Verfahren" nicht äußern. In die Wege geleitet hatte die Datensammlung ohne Widerspruchsmöglichkeit der ehemalige Gesundheitsminister Jens Spahn mit dem 2019 in Kraft getretene Digitale-Versorgung-Gesetz (DVG) (Koch, Datenschutz: Daten von Millionen Krankenversicherten können weitergegeben werden, www.heise.de 30.09.2022, Kurzlink: https://heise.de/-7279249).

Bundesweit

Erfassung der ukrainischen Kriegsflüchtlinge mit Spezialanwendung

Das Bundesamt für Migration und Flüchtlinge (BAMF) unterstützt alle 16 Bundesländer mit 180 Registrierungsstationen und über 270 Mitarbeitenden (Stand 11.05.2022) bei der erkennungsdienstlichen Erfassung der Flüchtlinge aus der Ukraine, vor allem Frauen und Kinder, und erhebt Fingerabdrücke, Personendaten und Fotos. Mit der seit dem 02.05.2022 im Einsatz befindlichen IT-Anwendung FREE sollen familiäre Bindungen bei der Verteilung der Menschen auf die Bundesländer berücksichtigt und Familien zusammengeführt werden.

Ein Großteil der Ankommenden kommt zwar aktuell privat unter, beispielsweise bei Verwandten, Bekannten oder freiwillig Unterstützenden. Personen, die eine Unterkunft benötigen und auf staatliche Leistungen angewiesen sind, werden auf die Bundesländer nach dem Königsteiner Schlüssel verteilt. Das BAMF ist dann nach § 24 Abs. 3 AufenthG zuständig für die Verteilung der Geflüchteten auf die Bundesländer. Die Fachanwendung FREE ist hierzu vor dem Hintergrund der Ukrainesituation neu entwickelt worden. Damit wurde auch eine Forderung des Deutschen Städtetages direkt erfüllt. Zuvor erfolgte die Verteilung von Personen, die ein Schutzgesuch nach § 24 AufenthG geäußert haben, über das EASY-System für die Erstverteilung von Asylsuchenden. „FREE" steht für „Fachanwendung zur Registerführung, Erfassung und Erstverteilung zum vorübergehenden Schutz". Das Verfahren bietet die Möglichkeit individuelle Rahmenbedingungen der Geflüchteten, wie z.B. familiäre

Bindungen, bei der Verteilung zu berücksichtigen.

Ukrainische Staatsangehörige mit biometrischem Reisepass halten sich nach derzeitigen EU-Regelungen für 90 Tage legal in Deutschland auf. Nach Ablauf des 90sten Tages des Aufenthalts bzw. bei Bedarf nach Bezug von Leistungen müssen sich die Personen registrieren lassen. Um eine überproportionale Unterbringung in Gebieten wie Hamburg oder Berlin zu vermeiden, soll FREE „personenscharfe und gleichzeitig lastengerechte Verteilung von Kriegsflüchtlingen aus der Ukraine unter Berücksichtigung integrationsförderlicher Bindungen" ermöglichen. Die Anwendung wurde vom BAMF selbst in enger Abstimmung mit allen Ländern designt. Anders als bei EASY wird eine Steuerungswirkung erreicht, da Personendaten und Verteilung miteinander verknüpft werden und in FREE durch eindeutige Identifizierungsmerkmale jederzeit nachverfolgbar sind. Die Zuständigkeit des ausgewählten Landes wird festgelegt und ist schon in der individuellen Anlaufbescheinigung erkennbar, die das Produkt des Vorgangs ist.

FREE wird auf Landesebene von den zuständigen Ausländerbehörden und Aufnahmeeinrichtungen genutzt; das BAMF stellt die IT-Fachanwendung zur Verfügung und hostet diese. Das webbasierte FREE kann über die aktuellen Browser Mozilla Firefox, Apple Safari, Google Chrome oder Microsoft Edge durch einen berechtigten Personenkreis aufgerufen werden. Die ebenso webbasierte Benutzerverwaltung erfolgt über ein delegiertes Verwaltungssystem, mit dem die beteiligten Stellen in Ländern und Kommunen selbst die Rechtevergaben gemäß Berechtigungskonzept realisieren können.

Die Erteilung des Aufenthaltstitels erfolgt weiterhin über die ausländerrechtlichen Fachverfahren. Die Ausstellung eines Aufenthaltstitels durch die zuständige Ausländerbehörde setzt voraus, dass die ukrainischen Kriegsflüchtlinge eine vollständige ED-Behandlung durchlaufen haben und ein Eintrag im AZR erfolgt ist.

In Vorbereitung ist eine Schnittstelle zum Ausländerzentralregister AZR, die eine unmittelbare Datenübertragung in FREE auf Basis des lesenden Zugriffs ermöglicht. Außerdem ist die automatisierte Dublettenprüfung geplant: Hierbei sollen automatisch identische Personendatensätze erkannt und zusammengeführt werden (IT-Fachanwendung: „FREE" im Einsatz, www.bamf.de 01.06.2022).

Berlin

Meike Kamp ist neue Datenschutzbeauftragte

Das Abgeordnetenhaus der Hauptstadt Berlin wählte am 06.10.2022 Meike Kamp zur neuen Chefin der dortigen Datenschutzaufsichtsbehörde. Die Stelle der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) war lange vakant. Die Juristin erhielt 94 von 123 Stimmen und damit auch Unterstützung aus der Opposition. Sie tritt die Nachfolge von Maja Smoltczyk an, die bereits am 27.10.2021 aus dem Amt geschieden war. Kommissarischer Leiter der Behörde war bisher Volker Brozio. Die rot-grün-rote Koalition brauchte – nicht nur aufgrund der Neuwahl des Abgeordnetenhauses im September 2021 – fast ein Jahr, um die Stelle neu zu besetzen. Auf Vorschlag der Grünen machte nun eine Expertin für E-Privacy, die Datenschutz-Grundverordnung (DSGVO) sowie Medien- und Informationsfreiheit das Rennen.

Kamp kennt die Behörde, die sie nun leiten soll, gut: Sie war von 2010 bis 2019 bei der BlnBDI tätig, zuletzt als Wirtschaftsreferentin. Zuvor hatte die 47-Jährige am Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein das Referat Datenschutz im nichtöffentlichen Bereich einschließlich Telemedien und Telekommunikation geführt. Zuletzt war sie für das Land Bremen als Sitzungsvertreterin im Rechts- und Innenausschusses des Bundesrates tätig. Als Dozentin und Referentin gibt Kamp Seminare zum Datenschutzrecht an Universitäten und bei Fachverbänden, darunter der Verbraucherzentrale Bundesverband (vzbv) und die Gesellschaft für Datenschutz und Datensicherheit (GDD).

Die Suche nach einer Nachfolgerin für Maja Smoltczyk war holprig verlaufen. Entsprechend erfreut zeigte sich Silke Gebel, Chefin der Grünen-Fraktion, die das Vorschlagsrecht für den Posten innehatte: „Uns allen war wichtig eine unabhängige Expertin zu bekommen." Die Sprecher für Datenschutz der Koalitionsfraktionen, Jan Lehmann (SPD), Stefan Ziller von den Grünen und Sebastian Schlüsselburg (Die Linke), gratulierten Kamp zur Wahl: „Mit der Besetzung erfüllen wir ein wichtiges innenpolitisches Anliegen des rot-grün-roten Koalitionsvertrages und schließen die Lücke in einem zentralen Ressort." Das Trio erklärte, dass in einer Stadt der Medien, Startups und Behörden wie Berlin „die Erwartungen an die Datenschutzbeauftragte hoch" seien.

Aus der Koalition soll zuvor die Hoffnung laut geworden sein, dass Kamp ihr Amt weniger restriktiv ausüben möge als Smoltczyk. Die Vorgängerin habe sich etwa wegen diverser Auseinandersetzungen während der Corona-Pandemie nicht sonderlich beliebt gemacht. In einem Kurztest der Aufsichtsbehörde waren weit verbreitete Videokonferenzsysteme wie Microsoft Teams, Skype, Zoom, Google Meet, GoToMeeting und Webex durchgefallen. Senat, Abgeordnetenhaus und Berliner Hochschulen setzten trotzdem weiter Lösungen von der schwarzen Liste ein und ignorierten Warnungen der Datenschützerin. Zudem hatte Smoltczyk wiederholt Verstöße bei der Polizei Berlin gerügt.

Als entscheidende Aufgabe im Bereich der Informationsfreiheit gilt es für Kamp die Arbeiten an einem Berliner Transparenzgesetz zu begleiten, das diesen Namen auch verdient. Ein erster Anlauf dazu scheiterte in den vergangenen Jahren an vorgesehenen breiten Ausnahmen für ganze Verwaltungsbereiche. 2021 hatten sich Betroffene in insgesamt 5.671 Fällen mit einer Beschwerde oder einem Beratungsersuchen an die BlnBDI gewandt, was einen Rekord darstellte. Einen weiteren Höchstwert gab es bei den Datenpannen: Hier meldeten private und öffentliche Stellen insgesamt 1.163 Vorkommnisse. Die Behörde sprach im Jahr 2021 212 Verwarnungen, zwei Warnungen und eine Anordnung aus. Zudem verhängte sie 61 Bußgelder in Höhe von insgesamt 133.350 Euro. Das höchste von Smoltczyk verhängte Bußgeld betrug 14,5 Millionen Euro. Der Bescheid richtete

sich gegen die Deutsche Wohnen. Der Immobiliengesellschaft gelang es aber, die Strafe vor Gericht wegen Verfahrensmängeln abzuwenden (Kiesel, Nach fast einjähriger Vakanz: Meike Kamp wird Datenschutzchefin in Berlin, www.tagesspiegel.de 13.09.2022; Krempl, Meike Kamp: Hohe Erwartungen an neue Berliner Datenschutzbeauftragte, www.heise.de 07.10.2022, Kurzlink: https://heise.de/-7287537).

Berlin

Unzulässige Polizeidatenbankabfragen führen zu Sanktionen

Aus einer Antwort des Berliner Senats auf eine Anfrage der Linken geht hervor, dass einzelne Berliner Polizisten in ihren internen Computersystemen immer wieder unberechtigt persönliche Daten von Bürgerinnen und Bürgern abfragen. In den vergangenen Jahren wurden aus diesem Grund jeweils zwischen 15 und 24 Ermittlungsverfahren eingeleitet. In der ersten Jahreshälfte 2022 gab es bereits 10 Ermittlungen wegen solcher Verstöße gegen den Datenschutz. In vielen Fällen wurden Bußgelder gegen die Polizisten verhängt, ein Teil der Ermittlungen wurde eingestellt. Die Betroffenen, also die Menschen, deren Daten abgefragt wurden, seien „in der überwiegenden Zahl von Fällen benachrichtigt" worden. Zugriffe auf die Datenbank der Polizei POLIKS (Polizeiliches Landessystem für Information, Kommunikation und Sachbearbeitung) werden intern protokolliert und sind so rückwirkend festzustellen (Polizei Berlin fragt Privates ab, SZ 10.08.2022, 8).

Niedersachsen

Thiel warnt vor Werbeprofiling bei Banken

Die Landesbeauftragte für den Datenschutz (LfD) Niedersachsen, Barbara Thiel, warnte nach der Prüfung einer Genossenschaftsbank, die als Pilotbank sogenannte Smart-Data-Verfahren testet, die anderen 89 genossenschaftlichen Banken in Niedersachsen vor dem Einsatz solcher Verfahren.

Bei dem Smart-Data-Verfahren wurden aus dem Kundenbestand gezielt Personen für bestimmte Werbemaßnahmen herausgefiltert, indem Scorewerte berechnet werden über die Wahrscheinlichkeit des Interesses an einem bestimmten Produkt, etwa an einem Immobilienkredit, einer Kreditkarte oder einem Wertpapiersparplan. Anschließend erhält die Kundin oder der Kunde Werbung für das entsprechende Produkt. Zur Bildung der Scorewerte werden unter anderem Zahlungsverkehrsdaten analysiert und bei einigen Verfahren auch Daten über das Wohnumfeld der Kundinnen und Kunden von externen Dienstleistern hinzugezogen.

Zur Berechnung, ob jemand Interesse an einem Konsumentenkredit hat, wurden z.B. 162 Datenfelder genutzt, darunter folgende Informationen aus dem Zahlungsverkehr: Bezug von sozialen Leistungen, Ausgaben für Haushalt und Lebensmittel, Höhe der Fahrzeugkosten, Höhe der „Grundkosten", u.a. für Energieversorger, Höhe des Gehalts- oder Renteneingangs, Höhe der Auszahlungen an Geldautomaten, Umsätze in der Kategorie E-Payment, z.B. Paypal und Amazon.

Zudem wurden von externen Dienstleistern Daten zum Wohnumfeld angekauft und in die Berechnung eingeführt, z.B. Anteil der Bevölkerung mit Realschulabschluss, durchschnittliche Anzahl der Kinder pro Haushalt, durchschnittliche Anzahl der Personen pro Haushalt, Nettoeinkommen der Haushalte, durchschnittliche private Kaufkraft für Hypothekendarlehen, Konsumentenkredite, Lebensversicherungen und private Krankenversicherungen, Anteil der Bevölkerung mit Familienstand „geschieden".

Die Aufsichtsbehörde hält eine solche Verarbeitung mangels überwiegendem berechtigten Interesse und mangels wirksamer Einwilligung für rechtswidrig. Die Durchführung von Verhaltensprognosen auf Grundlage von Zahlungsverkehrsdaten entspräche nicht den vernünftigen Erwartungen der Kundschaft. Bereits in einem anderen Fall hatte die LfD Niedersachsen im Juli 2022 ein Bußgeld von 900.000 Euro verhängt, weil eine Bank die Grenzen der Interessenabwägung bei der Verarbeitung personenbezogener Daten für Werbezwecke überschritten hatte.

Die Einwilligungsformulare wurden beanstandet, weil die Kunden nicht selbst entscheiden können, ob und welche konkreten Smart-Data-Verfahren durchgeführt werden. Sie konnten nur allgemein in die Profilbildung für Werbezwecke einwilligen ohne dabei steuern zu können, in welchem Umfang dies geschieht. Thiel erklärte: „Zahlungsverkehrsdaten sind sehr sensibel, weil sie Informationen über das Konsumverhalten, Beziehungen zu anderen Menschen, die wirtschaftliche Lage und persönliche Vorlieben enthalten. Sie ermöglichen so eine Vielzahl von Rückschlüssen auf das berufliche und private Leben der Betroffenen. Es muss deshalb sichergestellt sein, dass die betroffenen Personen die Kontrolle über die Verarbeitung dieser Daten ausüben können" (LfD Nds. PE v. 08.09.2022, LfD Niedersachsen warnt genossenschaftliche Banken vor Profilbildung für Werbezwecke).

Nordrhein-Westfalen

Palantir im umstrittenen polizeilichen Einsatz

Mitte 2019 suchte das Landeskriminalamt Nordrhein-Westfalen (LKA NRW) einen Anbieter für eine neue Software, mit der Informationen aus verschiedenen Datenbanken miteinander verknüpft werden können, um damit Fälle von Terrorismus und schwerer Kriminalität zu verhindern. Der Auftragswert laut Ausschreibung betrug 14 Millionen Euro. Die Ausschreibung gewonnen hat das höchst umstrittene Unternehmen Palantir. Die Firma ist eng verflochten mit US-Geheimdiensten. Ein Teil des Gründungskapitals kam von der CIA. Mit aufgebaut wurde die Firma von Milliardär und Trump-Unterstützer Peter Thiel.

Die Software soll aus Ermittlersicht den Vorteil haben, dass die verfügbaren Datenbanken nicht händisch durchsucht werden müssen. Mit ein paar Klicks übernimmt dies das Programm, so NRW-Innenminister Herbert Reul: „Das ist gar keine Zauberwaffe, sondern was ganz Banales." Aus Datenschutzsicht ist die Software problematisch: Palantir

kann nicht nur auf die Datenbanken der Polizei zugreifen, sondern auch andere Informationen einbeziehen, etwa aus dem Waffenregister, dem Einwohnermeldeamt oder der Führerscheinstelle. Ermittler haben sogar die Möglichkeit im Einzelfall Daten aus Social-Media-Kanälen wie Facebook und Internetdaten hinzuzufügen.

Mehrere Polizeibehörden wie Europol oder die New Yorker Polizei stellten nach anfänglicher Begeisterung die Zusammenarbeit mit Palantir wieder ein. Grund sollen unter anderem stark steigende Kosten gewesen sein.

Das Innenministerium Nordrhein-Westfalen räumte jetzt ein, dass die Behörden weit mehr zahlten als den in der Ausschreibung genannten Auftragswert von 14 Millionen Euro. Insgesamt 22 Millionen Euro netto sollen demnach als Lizenzkosten für fünf Jahre die Zahlungen an Palantir betragen.

Das Ministerium teilte weiter mit, im Ausschreibungsverfahren habe sich gezeigt, dass die geforderten Leistungen nicht für den geschätzten Wert erbracht werden konnten. Die Angebote lagen demnach alle „über 20 Millionen Euro – zum Teil deutlich". Nach Vertragsabschluss sei der Wert nicht mehr verändert worden. Doch die Kosten stiegen weiter. Alleine für zusätzliche Hardware sollen rund 2,4 Millionen Euro aufgewendet worden sein. In Summe seien 13 Millionen Euro „für ergänzende Tätigkeiten anderer Unternehmen ausgegeben" worden. In beiden Fällen möchte das Ministerium „aufgrund vertraglicher Verpflichtungen" keine konkreten Empfänger oder Leistungen mitteilen. Mittlerweile kostet das Gesamtprojekt das Land NRW insgesamt 39 Millionen Euro.

Im NRW-Landtag kannten die Abgeordneten diese Zahl bisher nicht. Hartmut Ganzke (SPD) erinnert sich, dass er im März 2021 noch überrascht war. Das Innenministerium hatte versucht 7 Millionen Euro für die Software als Corona-Mehrkosten bewilligt zu bekommen: „In der Rückschau kann man vielleicht sagen, dass der Minister versucht hat zu tricksen, dass er uns die notwendigen Informationen nicht an die Hand gegeben hat." Innenminister Reul nannte das einen Fehler, verneinte aber eine Täuschungsabsicht. In Bezug auf die Anschaffung der Palantir-Software hat es nach Reul keine Kostensteigerungen gegeben: „Palantir ist nicht teurer geworden, sondern wir haben falsch eingeschätzt und wir haben nachher sauber die Leistungen dazugerechnet, die nicht Palantir sind, die aber zu dem Projekt dazu gehören."

Marc Lürbke (FDP) war zum Zeitpunkt der Entscheidung für Palantir noch Teil der Regierungskoalition im Landtag. Doch auch er fühlt sich bis heute nicht ausreichend informiert, hat nach eigenem Bekunden keine Kenntnisse darüber, wie die Verträge mit dem US-Unternehmen ausgestaltet wurden oder welche Kosten dem Steuerzahler in Zukunft noch entstehen: „Ich würde mir wünschen, der Innenminister würde hier für Transparenz sorgen."

Einen Teil der Millionen erhielt Palantir aus NRW, ohne dass die Software überhaupt schon zum regulären Einsatz kam. Mehr als anderthalb Jahre lief das System nur in einem Testbetrieb. Die rechtliche Grundlage, um das System zu nutzen, war ungeklärt. Innenminister Reul meinte zunächst, dass kein neues Gesetz nötig sei. Noch im November 2020 wiederholte er vor dem Innenausschuss, die Landesregierung habe „alles Mögliche datenschutzrechtlich überprüft, weil sie wohl kaum ein rechtlich nicht sicheres Projekt starte". Dies gelte sowohl für die Vergabe als auch für den Datenschutz.

Das Büro der NRW-Datenschutzbeauftragten drängte allerdings auf eine neue rechtliche Regelung; Reul änderte seine Haltung. Im April 2022 beschloss der Landtag ein neues Polizeigesetz, das den Einsatz der Datenbanksoftware ausdrücklich erlaubt.

Statt wie in der Ausschreibung gefordert, ab dem dritten Quartal 2020 die Software bei Ermittlungen einzusetzen, konnte Palantir erst Anfang Mai 2022 für die reguläre Benutzung freigegeben werden. Die Weigerung des Innenministeriums die Datenschutzbehörde früher einzubinden, könnte den Steuerzahler so Millionen gekostet haben. Denn die Zahlungen von jährlich bis zu 6,8 Millionen Euro liefen bereits.

Bettina Gayk, die Landesbeauftragte für Datenschutz in NRW, meinte: „Man hätte uns früher einbeziehen sollen." Zum Zeitpunkt der Auftragsvergabe an Palantir war sie noch nicht im Amt. Mit dem neuen Polizeigesetz sieht sie gewährleistet, dass die Software nicht bei Bagatelldelikten eingesetzt wird: „Die Frage ist aber: Wie wird das in der Praxis gewährleistet?" Dafür soll zeitnah ein Kontrolltermin im LKA organisiert werden, „weil das einfach so ein gravierendes Verfahren ist, dass es wichtig ist, dass das in engen Bahnen bleibt".

Reul beschreibt den Einsatz der Software als vollen Erfolg. Es seien schon mehrfach Straftaten damit verhindert worden, etwa Geldautomatensprengungen und auch sexualisierte Gewalt an Kindern: Die Polizei nutzt laut Ministerium das System inzwischen täglich. Es ist umstritten, ob die Regelungen in NRW die Grundrechte tatsächlich ausreichend schützen. Jürgen Bering, Bürgerrechtler bei der Gesellschaft für Freiheitsrechte (GFF), erklärte: „Es muss viel klarer werden, was ist die Schwelle, welcher Verdacht muss eigentlich schon bestehen, ab dem die Software eingesetzt werden kann." Die Software sei in der Lage Data-Mining zu betreiben also selbst neue Informationen aus den abgefragten Daten zu erzeugen, was nur bei schwersten Straftaten erlaubt sei, etwa Terrorismus oder Kindesmissbrauch. Das NRW-Gesetz lässt den Einsatz der Software dagegen auch bei Straftaten wie Betrug, Beamtenbestechung oder Volksverhetzung zu.

Das Innenministerium bestreitet, dass die Polizei mit der Software Data-Mining betreibe. Die GFF kündigte eine Verfassungsbeschwerde an. Letztlich dürfte also das Bundesverfassungsgericht entscheiden, ob die Polizei in NRW die Palantir-Software weiter wie bisher nutzen darf (Hell/Kartheuser, NRW-Polizei: Knapp 40 Millionen Euro für umstrittene Palantir-Software, www1.wdr.de 25.09.2022).

Rheinland-Pfalz

Kirchliche Geheimhaltung schützt Täter und stellt Opfer bloß

Im Auftrag von Karin Weißenfeld (Pseudonym, im weiteren Text K.W.) hat der Bamberger Kirchenrechtsanwalt Friedolf Lappen den Trierer Bischof Stephan Ackermann wegen des

indirekten Bruchs des Beichtgeheimnisses bei Papst Franziskus angezeigt. K.W. ist, wie die unabhängige Aufarbeitungskommission im August 2022 festgestellt hat, Opfer sexuellen Missbrauchs. Ackermann war seit 2010 der Missbrauchsbeauftragte der deutschen Bischofskonferenz. K.W. arbeitete seit Ende der 80er Jahre als Gemeindereferentin mit ihrem Chef J.D. zusammen, ein mehr als 20 Jahre älterer Priester. Die 30jährige, streng katholisch erzogene K.W. war sexuell völlig unerfahren. Sie wurde von J.D. missbraucht, konnte sich aber nicht wehren. Nach einigen Monaten wurde sie schwanger; J.D. trieb sie zum Schwangerschaftsabbruch, doch K.W. wollte – im Sinne der katholischen Lehre – das Kind austragen. Sie offenbarte in einer Beichte dem Geistlichen M.B., einem guten Freund von J.D., dass sie aus der Arztpraxis davongelaufen sei, doch der drängte sie auch zur Abtreibung, so dass sie doch von den beiden Geistlichen zur Abtreibung gebracht wurde. J.D. beschwörte K.W. von der Abtreibung niemandem zu erzählen, missbrauchte sie aber – gemäß den Angaben von K.W. – weiterhin viele Jahre lang fast täglich. J.D. beichtete dies seinem Freund M.B. telefonisch, der ihn von seinen Sünden immer wieder lossprach: „Ego te absolvo – ich spreche dich los von deinen Sünden."

Erst nach vielen Jahren konnte sich K.W., die beruflich und emotional von J.D. abhängig war, von diesem lösen. Im Buch „Erzählen als Widerstand" schildert sie unter ihrem Pseudonym „Karin Weißenfels" ihr Martyrium, möchte aber, da sie weiterhin im Bistum arbeitet, nicht, dass ihr Klarname bekannt wird. Dessen ungeachtet offenbarte Bischof Ackermann während einem Online-Hearing zu Fällen sexueller Gewalt ihren wirklichen Namen, so dass mindestens 40 Mitarbeitende des Bistums die Vorgänge ihrer Person zuordnen können.

K.W.s Anwalt Oliver Stegmann legte daraufhin Beschwerde bei der katholischen Datenschutzstelle ein, hörte aber bis Ende September 2022 von dieser nichts über eine Entscheidung. Der Kirchenrechtsanwalt Friedolf Lappen wendete sich daraufhin wegen der Verletzung des Beichtgeheimnisses an den Papst.

Kirchenrechtlich ist der Beichtgeheimnisbruch ein schweres Vergehen, das bis zur Exkommunikation geahndet werden kann. Aus Rom gab es bis Ende September 2022 keine Antwort.

In dem Fall spielt der heutige Erzbischof von München und Freising Kardinal Reinhard Marx, der Vorgänger von Bischof Ackermann in Trier, eine Rolle. Er führte mit K.W. mehrere Gespräche, doch erst als die Frau einen Kirchenrechtler einschaltete, passierte nach Jahren etwas. Marx ließ J.D. im Jahr 2004 und drei Jahre später den Beichtpriester M.B. für irregulär erklären wegen der „positiven Mitwirkung an einer Abtreibung". Kurz darauf begnadigte die Kleruskongretation im Vatikan J.D.; Marx hatte J.D. auf diese Möglichkeit hingewiesen. Auch M.B. wurde begnadigt. Der Vorwurf des sexuellen Missbrauchs, den K.W. schon im Januar 2003 erhob, wurde straf- oder kirchenrechtlich nie untersucht und verfolgt, obwohl J.D. seine Schuld gegenüber K.W. vollumfänglich eingestanden hatte. Im Dezember 2021 erfuhr K.W., dass J.D. sowohl den Rat zur Abtreibung wie auch die sexualisierte Gewalt offiziell gegenüber dem Bistum geleugnet hatte. Wenig später, ohne dass noch eine weitere Aufklärung möglich war, starb J.D. In den Zwischenbericht der unabhängigen Aufarbeitungskommission zum Handeln der Bistumsverantwortlichen wurde der Fall von K.W. nicht aufgenommen. Eine wirkliche Ahndung all der Verstöße – einschließlich der Verletzungen des Beichtgeheimnisses – blieb aus. K.W. erinnert sich, dass Ackermann ihr, wohl um sie zu trösten, gesagt habe, M.B. sei ja wenigstens nicht Bischof geworden. Sie bleibt gegenüber Bistumsmitarbeitenden bloßgestellt (Zoch, Schnell vergeben, nicht aufarbeiten, SZ 24./25.09.2022, 6).

Sachsen-Anhalt

Wahl des Datenschutzbeauftragten erneut gescheitert

Die schwarz-rot-gelbe Koalition in Sachsen-Anhalt scheiterte am 13.10.2022 erneut an der Wahl eines Datenschutzbeauftragten. Landtagspräsident Gunnar Schellenberger musste schon kurz nach Beginn der Landtagssitzung verkünden, dass es auch nach vier Jahren und im fünften Anlauf nicht gelungen war einen Datenschutzbeauftragten zu wählen: „Es gibt keinerlei Aussicht auf Erfolg. Aus diesem Grund beende ich hiermit das Verfahren."

Das Desaster für den Datenschutz in dem Land ist zugleich eine Belastungsprobe für die schwarz-rot-gelbe „Deutschland-Koalition", nachdem die CDU-Fraktion dem Kandidaten eine krachende Abstimmungsniederlage bescherte. Ganze 16 Ja-Stimmen von der Fraktion bekam Albert Cohaus, der seit zwei Jahren fachlich anerkannt interimsmäßig die Geschäfte des Landesdatenschutzbeauftragten führt. 51 Abgeordnete stimmten mit Nein, elf enthielten sich. 49 Stimmen wären für die Wahl nötig gewesen; CDU, SPD und FDP kommen zusammen auf 56, die CDU ist mit 40 Sitzen stärkste Fraktion.

Rein rechnerisch könnte CDU-Ministerpräsident Reiner Haseloff allein mit der SPD regieren; er formte aber im Sommer 2021 ein Dreierbündnis mit der FDP, weil er sich der Unterstützung seiner CDU-Fraktion nicht immer sicher sein konnte. Den strikten Abgrenzungskurs zur AfD beispielsweise finden dort nicht alle richtig. So offen wie bei dieser Datenschützerwahl zeigte sich der Widerstand aber bislang nicht. Noch Anfang der gleichen Woche, am Montag, hatte Fraktionschef Guido Heuer Unterstützung für Cohaus signalisiert: „Ich gehe davon aus, dass wir einen Datenschutzbeauftragen wählen werden." Am Mittwoch erklärte Heuer dann überraschend, die Abstimmung in der CDU-Fraktion sei freigegeben. Damit stand das zweite Scheitern von Cohaus praktisch fest. Im März 2022 hatten ihm nur drei Stimmen zur Mehrheit gefehlt. Seitdem wird spekuliert, dass Teile der CDU-Fraktion lieber einen Parteifreund statt eines Experten im Amt sähen. Die Nichtwahl eines Datenschutzbeauftragten hat in Magdeburg schon Tradition: Dreimal verfehlte 2018 der Kandidat der damaligen „Kenia-Koalition" die nötige Mehrheit (DANA 2/2018, 108 f.).

Bundesdatenschutzbeauftragter Ulrich Kelber äußerte sich frustriert: „Es macht mich fassungslos. Dieser Verstoß gegen die Datenschutz-Grundverord-

nung ist in der gesamten Europäischen Union ohne Vergleich." Es sei nicht auszuschließen, dass die EU-Kommission nun ein Vertragsverletzungsverfahren gegen Deutschland einleite. Der parlamentarische Geschäftsführer der Grünen-Fraktion, Sebastian Striegel, meinte: „Dass Ministerpräsident Haseloff dabei zuschaut, wie sein Fraktionsvorsitzender die zahlenmäßig überaus komfortable Regierungsmehrheit schrotet, ist ein auch für CDU-Maßstäbe beeindruckender Tiefpunkt von Führungslosigkeit." Die Koalition gestalte nichts mehr: „Ihre Mehrheit reicht nur noch zum Nein." Linken-Fraktions-Chefin Eva von Angern sprach von einem inakzeptablen Debakel: „Sie sollten darüber nachdenken, ob sie würdig sind, eine Regierung zu tragen."

FDP und SPD zeigten sich enttäuscht. SPD-Fraktionschefin Katja Pähle sagte: „Es ist ein Trauerspiel, dass es im Landtag von Sachsen-Anhalt nicht möglich ist wie in allen anderen Landtagen einen Datenschutzbeauftragten zu wählen." Man werde nun in der Koalition nach Lösungen suchen. Cohaus selbst gab sich gefasst: „Man ist da als Bewerber zwischen den politischen Fronten." Die Geschäfte werde er weiter interimsmäßig führen. Seine altersbedingte Pensionierung steht im April 2025 an (Mayer, Belastungsprobe für Schwarz-Rot-Gelb, SZ 14.01.2022, 5).

Schleswig-Holstein

QR-Code-Versendung für E-Rezept ist personenbezogen

Die Landesdatenschutzbehörde Schleswig-Holstein, das Unabhängige Landeszentrum für Datenschutz (ULD), hat die Einführung von QR-Codes im Rahmen des E-Rezepts gestoppt. Das Versenden des Codes per SMS oder E-Mail stellt laut dem ULD eine Übermittlung von Patientendaten dar. Wenn die Mails mit dem Code nicht Ende-zu-Ende-verschlüsselt sind, sei das Versenden unsicher. Auch Apps zur Übermittlung seien nicht sicher: „Dabei ist zu berücksichtigen, dass auf dem Markt frei erhältliche Apps aus dem Apothekenumfeld jeder Person, die befugt oder unbefugt im Besitz des QR-Codes ist, die Kenntnisnahme von Daten einer Verordnung ermöglicht." Für einen Missbrauch dieser Daten könnten potentiell die ausstellenden Ärzte in Haftung genommen werden. Auch eine Zustimmung der Patienten für die Übermittlung an sie oder an eine Apotheke ändere nichts an dieser Bewertung.

Die QR-Codes für E-Rezepte werden generiert, wenn die Praxisverarbeitungssoftware (PVS) einer Arztpraxis ein Rezept ausstellt. Das wird über die Telematikinfrastruktur (TI) an die Gematik geleitet, die für die TI zuständig ist. Der dem Patienten oder der Patientin bereit gestellte QR-Code kann dann von Apotheken gescannt werden, sodass die benötigten Daten, wie Name, Adresse, Versichertennummer, Krankenkasse, ausstellende Praxis, Rezept und Dosierung, sichtbar werden, ebenso wie auf einem analogen Rezept. Im Gegensatz zum Papierrezept seien aus einem QR-Code zwar keine der obengenannten Daten ersichtlich, so das ULD. Nach einem Scan sei das aber der Fall, weshalb das nicht verschlüsselte Verschicken des Codes nicht zulässig sei. Das sei unsicherer als ein Papierrezept, über das die Patienten physisch verfügten.

Eigentlich sollten ab September 2022 alle Apotheken in der Lage sein E-Rezepte einzulesen. Praxen sollen erst nach und nach regional verpflichtet werden.

Die ehemalige Beauftragte der Bundesregierung für die Belange der Patientinnen und Patienten und Bundestagsabgeordnete Claudia Schmidtke (CDU) kommentierte den Vorgang: „Dass das E-Rezept vom Landesdatenschutz in SH gekippt wird, zeigt, wie weit wir vom digitalen Gesundheitswesen in Deutschland entfernt sind." Laut Mitteilung der Kassenärztlichen Vereinigung Schleswig-Holstein (KVSH) würden durch die Bewertung aus Schleswig-Holstein 99% aller digitalen Übermittlungswege unmöglich. Auch die App der Gematik ist in den meisten Fällen noch nicht nutzbar, weil die Patienten unter anderem NFC-fähige Karten brauchen, um die E-Rezept-App nutzen zu können. Die seien allerdings aufgrund des aktuellen Chipmangels auch Mangelware.

Das ULD wehrte sich gegen die Behauptung, es habe das E-Rezept in Schleswig-Holstein untersagt. In der erst im Juli 2022 erbetenen Beratung der KVSH hatte das ULD auf das Risiko des E-Mailversands hingewiesen und mehrere mögliche Lösungen aufgezeigt: Anstelle der E-Rezept-App oder des Ausdrucks kämen beispielsweise die Nutzung des Systems „Kommunikation im Medizinwesen" (KIM) oder ein digitaler Versand z. B. per E-Mail mit zusätzlicher Ende-zu-Ende-Verschlüsselung infrage. Dadurch verbleibe den Patienten die Verfügungsgewalt über ihre Daten. Die Landesbeauftragte für Datenschutz und ULD-Chefin Marit Hansen erläuterte: „Wer auf eine unsichere Alternative setzt, verursacht damit ein Risiko für die betroffenen Personen und würde sogar den Anreiz nehmen die zu diesem Zweck entwickelten Systeme mit einem angemessenen Schutz einzusetzen." (Datenschützer stoppen E-Rezept in Schleswig-Holstein, Tagesspiegel Digitalisierung & KI, 23.08.2022; ULD, E-Rezept-Verfahren: maschinenlesbare Codes schützen! PE v. 23.08.2022).

Datenschutznachrichten aus dem Ausland

Weltweit/China

Globaler digitaler Autoritarismus auf dem Vormarsch

Ende September 2022 haben der Iran, die Türkei, Myanmar und eine Handvoll weiterer Länder Schritte unternommen, um Vollmitglieder der sogenannten Shanghaier Organisation für Zusammenarbeit (SOZ, auf Englisch: SCO) zu werden, einer wirtschaftlichen wie politischen Allianz, die von den autoritären Regimen Chinas und Russlands angeführt wird. Die 2001 gegründete Gemeinschaft hat sich schnell zu einer der wichtigsten Kräfte in der Weltpolitik entwickelt, für die Technologie ein wichtiger Bestandteil ihrer strategischen Zukunft ist. Obwohl sich die SOZ

vor allem auf die regionale Entwicklung konzentriert, z.B. auf Eisenbahnlinien und Handelsabkommen, ist sie ein wichtiger Akteur bei der Verbreitung von Technik zur sozialen Kontrolle, die als „digitaler Autoritarismus“ bezeichnet werden kann. Mit der Türkei beabsichtigt erstmals ein NATO-Land der SOZ vollständig beizutreten.

Die Mehrheit der SOZ-Mitgliedsländer sowie andere autoritäre Staaten, die sich in ihrem Dunstkreis befinden, tendieren gemäß dem Vorbild China zu mehr digitalen Menschenrechtsverletzungen und praktizieren technische Massenüberwachung der Bürger, Zensur im Internet sowie eine Kontrolle der individuellen und journalistischen Meinungsäußerung.

Auch Demokratien setzen in großem Umfang Überwachungstechnik ein. In den Vereinigten Staaten kommt massiv Kameraüberwachung zum Einsatz, die ironischerweise vorrangig aus China kommt. Doch die technologischen Handelsbeziehungen zwischen autoritären Ländern überall auf der Welt – sowohl zwischen den Mitgliedern der OSZE als auch ihren Verbündeten – vertiefen sich zusehends. Diese Staaten nutzen ähnliche Spielregeln für eine digital gestützte soziale Kontrolle und kopieren einander.

• Berichte von Freedom House

2018 konzentrierte sich Freedom House, eine gemeinnützige Forschungs- und Interessensgruppe für globale Demokratie, auf den „Aufstieg des digitalen Autoritarismus“. Damals erschien ihr Jahresbericht über den Zustand der Freiheit im Internet. Darin steht: „Digitaler Autoritarismus wird als eine Möglichkeit für Regierungen begriffen ihre Bürgerinnen und Bürger durch Technologie zu kontrollieren – und stellt das Konzept des Internet als Motor der menschlichen Freiheit auf den Kopf.“ Die amerikanische Regierung hat mittlerweile diese Sichtweise übernommen und nennt als Hauptakteur China. Es besteht ein enger Zusammenhang zwischen Regierungssystemen und dem jeweiligen Stand der digitalen Rechte, wobei autoritäre Regime eher als demokratische Regime dazu neigen Technologie als weiteren Bereich für die soziale Kontrolle zu nutzen.

Die Forschenden von Freedom House versuchen dieses Phänomen in ihren Jahresberichten zu quantifizieren, indem sie die Länder nach einer Reihe von Faktoren bewerten, darunter dem Schutz der Privatsphäre, der Zensur und den Hindernissen, die es für einen freien Internetzugang gibt. Weltweit sind die Werte elf Jahren in Folge gesunken, was bedeutet, dass sich die Welt im Allgemeinen von einem Internet entfernt, das die digitalen Rechte der Nutzer schützt. Keines der nicht-demokratischen Länder wurde von Freedom House als eines mit „freiem“ Internet eingestuft, während alle demokratischen Länder entweder als „frei“ oder „teilweise frei“ bewertet wurden.

Alle acht derzeitigen Mitglieder der SOZ – China, Russland, Tadschikistan, Usbekistan, Kasachstan, Kirgisistan, Indien und Pakistan – schneiden schlecht ab. Ihre Werte sind in den letzten zehn Jahren um durchschnittlich 10 Punkte gefallen. China belegte im letzten Jahr den letzten Platz auf der Berichtskarte von Freedom House – wie jedes Jahr seit 2014. Iran, noch kein Vollmitglied der SOZ, belegte den vorletzten Platz. Seine wirtschaftlichen Beziehungen zu China haben sich in den letzten Jahren intensiviert und dies insbesondere auch bei digitaler Überwachungstechnologie.

• Die Rolle der USA und von China

Das Ausmaß des Exports von Autoritarismus durch China und die globale Rolle der USA hierbei sind umstritten. MIT Technology Review berichtete, wie sich eine Initiative des US-Justizministeriums, die chinesische Spione ausfindig machen sollte, zu einem großen Schlamassel entwickelt hat. Andere Untersuchungen weisen hingegen auf eine starke Nachfrage nach chinesischer Überwachungstechnologie in Ländern mit hoher Kriminalitätsrate hin – unabhängig davon, ob es sich um Demokratien handelt oder nicht. Es ist aber weitgehend unstreitig, dass der chinesische Staat über die SOZ und die sogenannte Belt and Road Initiative (BRI, „Neue Seidenstraße“), sein wichtigstes außenpolitisches Unternehmen, das die Entwicklung der Infrastruktur in über 140 Ländern fördern soll, über staatsnahe Unternehmen andere Länder mit Sicherheits- und Überwachungstechnologie umfassend ausstattet.

Chinas Einfluss auf den digitalen Autoritarismus ist kaum zu überschätzen. Seine öffentlichen und privaten Social-Credit-Programme, die erstmals 2014 angekündigt wurden, sammeln und aggregieren Daten über die Einkäufe, Verkehrsverstöße und sozialen Aktivitäten der Menschen. Die chinesischen Städte sind die am stärksten überwachten der Welt, mit mehr Kameras pro Quadratkilometer als irgendwo sonst. Diese Kameras sind häufig mit Gesichtserkennung und visueller Computeranalyse ausgestattet, was die Überwachung für den Sicherheitsapparat und die Kommunistische Partei erleichtert.

Die größten Projekte der SOZ werden in der Regel von China geleitet und finanziert; dazu gehören die transafghanische Eisenbahnlinie, die Usbekistan mit Pakistan verbindet, eine digitale Handelsplattform in Chongqing und gemeinsame Militärübungen. Aber es hat auch Initiativen wie das Programm „Thousand Cities Strategic Algorithms“ gefördert, das Zentralregierungen ermutigt große Datenmengen zur Entscheidungsfindung zu nutzen. Zwischen Januar und August 2022 stieg der chinesische Handel mit den SOZ-Ländern um 26% gegenüber dem Vorjahreszeitraum. Ein großer Teil dieses Volumens entfiel auf chinesische Exporte elektronischer Komponenten, einschließlich Datenverarbeitungstechnologien.

Außerhalb der SOZ kündigte das autokratische Regime Venezuelas 2017 einen „intelligenten Ausweis“ für seine Bürgerinnen und Bürger an, der mit Hilfe des chinesischen Telekommunikationsunternehmens ZTE Informationen über Beschäftigung, Wahlen und medizinische Versorgung zusammenfasst. Huawei, ein weiteres chinesisches Telekommunikationsunternehmen, verfügt laut Jahresbericht 2021 über ein globales Netzwerk von 700 Orten mit seiner hauseigenen Smart-City-Technologie. Dies ist ein Anstieg gegenüber 2015, als das Unternehmen etwa 150 internationale Verträge mit Städten hatte.

Auch Demokratien sind in den digitalen Autoritarismus verwickelt. Die USA verfügen über ein beeindruckendes Überwachungssystem, das auch auf chinesischer Technologie basiert.

Eine aktuelle Studie der Branchenforschungsgruppe Top10VPN ergab, dass über 700.000 US-Kameranetzwerke von den chinesischen Unternehmen Hikvision und Dahua betrieben werden (DANA 3/2022, 196 ff.).

US-Unternehmen sind oft Schlüsselakteure in komplexen Lieferketten, was eine Isolierung autoritärer Staaten oder auch nur eine Rechenschaftspflicht erschwert. So betreibt Intel beispielsweise angeblich Server für Tiandy, ein chinesisches Unternehmen, das für die Entwicklung von Hardware bekannt ist, die Berichten zufolge bei Folterungen eingesetzt wird. Der digitale Autoritarismus geht über Software und Hardware hinaus. Im weiteren Sinne geht es darum, wie der Staat die Technologie nutzen kann, um seine Kontrolle über die Bürger zu verstärken. Von staatlichen Akteuren verursachte Internet-Blackouts haben in den letzten zehn Jahren dauernd zugenommen. Die Fähigkeit eines Staates das Internet abzuschalten, ist an das Ausmaß seiner Verfügungsmacht über die Internet-Infrastruktur gebunden – ein Markenzeichen autoritärer Regime wie China und Russland. Und je wichtiger das Internet für alle Lebensbereiche wird, desto mehr können solche Blackouts zur Destabilisierung und zum Schaden der Menschen beitragen. Anfang 2022, als regierungsfeindliche Proteste Kasachstan, ein SOZ-Mitglied, erschütterten, schaltete der Staat das Internet fünf Tage lang fast vollständig ab. Während dieser Zeit rückten russische Truppen in Großstädte ein, um die Proteste zu unterdrücken. Der Blackout kostete das Land mehr als 400 Millionen Dollar und führte zur Unterbrechung wichtiger Dienste.

• Strategien

Zu den weiteren Taktiken gehören Modelle für die Nutzung von „Data Fusion“ und Künstlicher Intelligenz zur Verarbeitung von Überwachungsdaten. Während des SOZ-Gipfels 2021 veranstalteten chinesische Vertreter eine Podiumsdiskussion über die strategischen „Algorithmen der Tausend Städte“, in der den Zuhörern erklärt wurde, wie ein „nationales Datengehirn“ entwickelt werden kann, das verschiedene Formen von Finanzdaten integriert und Künstliche Intelligenz einsetzt, um sie zu analysieren und sinnvoll zu nutzen. Laut der SCO-Website führen 50 Länder „Gespräche“ mit der Initiative Thousand Cities Strategic Algorithms.

In diesem Zusammenhang verbreitet sich der Einsatz von Gesichtserkennungstechnologien weltweit, und auch die Investitionen in fortschrittliche Bildverarbeitung, die dabei helfen kann aus Kamerabildern sinnvolle Daten abzulesen, haben zugenommen, insbesondere in Russland. In seiner Rede auf dem SOZ-Gipfel im September 2022 ging der chinesische Präsident Xi Jinping so weit die globale Mentalität des Kalten Krieges und die zunehmend protektionistische Haltung gegenüber dem Handel anzuerkennen. Xi drängte darauf, dass Kooperationsabkommen „in Bereichen wie Handel und Investitionen, Aufbau von Infrastruktur, Schutz von Lieferketten, wissenschaftlichen und technologischen Innovation und Künstliche Intelligenz“ im Rahmen des Gipfels verabschiedet werden. Hierzu will er mehr Nationen in die chinesische Umlaufbahn bringen. Während er sich für die Werte des Friedens und des Multilateralismus einsetzte, forderte er „eine engere SOZ-Gemeinschaft mit einer gemeinsamen Zukunft“. Zu dieser Zukunft gehört auch die offizielle Verkündung eines neuen Bildungsprogramms des „China-SCO Institute of Economic and Trade“ an der Universität Qingdao, das im Januar 2022 begann und Studenten in SOZ- und BRI-Staaten in Themen wie wirtschaftliche Entwicklung und dem digitalen Handel schulen wird. (Dieses Programm baut auf früheren Schulungen auf, die China mit BRI-Ländern zum Management digitaler Medien durchgeführt hat.) Es gibt bisher wenig Initiativen, die das globale Wachstum des digitalen Autoritarismus aufzuhalten versuchen (Ryan-Mosley, Wie autoritäre Länder Überwachungstechnik aus China einsetzen, www.heise.de 26.09.2022, Kurzlink: https://heise.de/-7273169).

EU

EDSB klagt wegen Massenverarbeitung gegen Europol

Der EU-Datenschutzbeauftragte (EDSB) Wojciech Wiewiórowski beantragte am 16.09.2022 beim Europäischen Gerichtshof (EuGH) die Artikel 74a und 74b der jüngst geänderten Europol-Verordnung für nichtig zu erklären. Diese hätten den Effekt, „dass sie rückwirkend die Praxis des Europäischen Polizeiamts (Europol) legalisieren große Mengen an personenbezogenen Daten von Personen zu verarbeiten, ohne dass eine Verbindung zu einer kriminellen Aktivität nachgewiesen ist“.

Die kritisierte Europol-Verordnung ist Ende Juni 2022 in Kraft getreten, womit das Mandat für Europol deutlich erweitertet wird. Seine Ermittler dürfen danach künftig umfangreiche und komplexe Datensätze verarbeiten und mit Big-Data-Analysen die Mitgliedstaaten in ihrem Kampf gegen schwere Kriminalität und Terrorismus unterstützen. Vor allem nationale Strafverfolgungsbehörden wie das Bundeskriminalamt (BKA) oder die französische Nationalpolizei beliefern Europol schon seit Jahren mit großen Mengen an Daten. Der Datenspeicher des Polizeiamts umfasst Schätzungen zufolge spätestens mit dem Unterwandern der verschlüsselten Kommunikationsdienste Sky ECC und Encrochat mittlerweile insgesamt mindestens vier Petabyte.

2020 hatte Wiewiórowski gerügt, dass Europol-Ermittler mit dem Sammeln und Analysieren nicht mehr überschaubarer Datenmengen ihre Befugnisse überschreiten und rechtswidrig handeln. Unverdächtige wie Opfer, Zeugen oder Kontaktpersonen liefen damit Gefahr „unrechtmäßig mit einer kriminellen Aktivität in der gesamten EU in Verbindung gebracht zu werden“.

Der EDSB ordnete Anfang 2022 an, dass die Strafverfolgungsbehörde künftig binnen sechs Monaten entscheiden müsse, ob sie erhaltene personenbezogene Informationen längerfristig speichern und verwenden darf. Diese Auflage wurde mit dem novellierten Mandat weitgehend hinfällig.

Wiewiórowski stellt mit seiner Klage ernüchtert fest, dass die EU-Gesetzgeber beschlossen hätten „diese Art der Datenverarbeitung rückwirkend zu legalisieren“ und so seine Anordnung „außer Kraft zu setzen“. Er sehe sich daher gezwungen gegen die beiden Ar-

tikel vorzugehen. Es gelte die „Rechtssicherheit für Einzelpersonen in dem hochsensiblen Bereich der Strafverfolgung zu schützen“. Die Verarbeitung personenbezogener Daten bringe in diesem Bereich „schwere Risiken für die betroffenen Personen mit sich“.

Wiewiórowski will ferner sicherstellen, „dass der EU-Gesetzgeber im Bereich des Schutzes der Privatsphäre und des Datenschutzes, in dem der unabhängige Charakter der Ausübung der Durchsetzungsbefugnisse einer Aufsichtsbehörde Rechtssicherheit in Bezug auf die durchzusetzenden Vorschriften erfordert, nicht in unzulässiger Weise ‚die Zielpfosten verschiebt‘“. Er spart so nicht mit Kritik am Vorgehen des EU-Parlaments und der Mitgliedsstaaten.

Bei der Erhebung von Daten im Rahmen der früheren Europol-Verordnung konnten die Bürger Wiewiórowski zufolge zumindest davon ausgehen, dass Europol beim Erhalt ihrer personenbezogenen Daten verpflichtet sein würde, „innerhalb von sechs Monaten zu prüfen, ob eine Verbindung zu einer kriminellen Tätigkeit besteht“. Andernfalls sollten einschlägige Informationen – wie von ihm vorgeschrieben – in einem ersten Schritt spätestens am 04.01.2023 gelöscht werden. Die neuen Bestimmungen erlaubten es den Ermittlern aber die noch nicht gelöschten Daten trotz der Anordnung weiter zu verarbeiten: „Die Entscheidung der Mitgesetzgeber solche Änderungen einzuführen, untergräbt die unabhängige Ausübung der Befugnisse der Kontrollbehörden“. Die angefochtenen Bestimmungen schafften einen beunruhigenden Präzedenzfall: Behörden könnten damit „mögliche Gegenreaktionen des Gesetzgebers vorwegnehmen, die darauf abzielen ihre Aufsichtstätigkeiten je nach politischem Willen außer Kraft zu setzen“. Kontrolleure könnten so gezwungen werden „politische Präferenzen zu berücksichtigen“. Es wäre möglich sie „ungebührlichem politischen Druck“ auszusetzen, was „ihre in der EU-Grundrechtecharta verankerte Unabhängigkeit untergräbt“.

Europol selbst beschreibt ihre neuen Kompetenzen wie folgt: Man sei nun in der Lage „personenbezogene Daten ohne die Kategorisierung der betroffenen Person zu verarbeiten, solange und wann immer dies für die Unterstützung einer bestimmten laufenden strafrechtlichen Ermittlung erforderlich ist“. Dies spiele vor allem für den Umgang mit großen und komplexen Datensätzen eine wichtige Rolle, die erst kategorisiert werden könnten, „wenn die relevanten Informationen extrahiert und analysiert“ worden seien (Krempl, EU-Datenschützer klagt gegen Europol-Befugnis zur Massenüberwachung, www.heise.de 22.09.2022, Kurzlink: https://heise.de/-7272715).

EU

Bürgerrechtliche Kritik an Prüm-Erweiterungen

Zivilgesellschaftliche Organisationen aus dem Netzwerk European Digital Rights (EDRi) befürchten gemäß einem am 07.09.2022 veröffentlichten 30-seitigen Positionspapier, dass über die Initiative der EU-Kommission für eine Verordnung „über den automatisierten Datenaustausch für die polizeiliche Zusammenarbeit“ die Unschuldsvermutung ausgehebelt wird. Damit würde der Prümer Vertrag deutlich ausgebaut und über die Forderungen des EU-Ministerrats weiter verschärft. Das Vorhaben öffne den Weg zur Massenüberwachung europäischer Bürger und Einreisender.

Der Prüm-Rahmen ermöglicht Polizeibehörden in den angeschlossenen Mitgliedsstaaten bereits seit Längerem DNA-, Fingerabdruck- und Fahrzeugregisterdaten elektronisch auszutauschen und abzugleichen. Einschlägige nationale Datenbanken können hierüber vernetzt werden. Laut der Kommission sollen künftig auch Fahndungsfotos oder biometrische Lichtbilder aus Polizeiregistern einbezogen werden, die eine automatisierte Gesichtserkennung unterstützen.

Geht es nach dem EU-Rat, soll die Zahl der nutzbaren Datenkategorien noch mehr erweitert werden, z.B. um Führerscheindaten und Akten von Verdächtigen sowie von überführten Straftätern. Zudem zielt der Rat auf einen automatisierten EU-weiten Abgleich aller DNA-Profile der Polizeibehörden der Mitgliedsländer untereinander sowie mit Europol ab. Bislang war nur ein manueller Abruf personenbezogener Informationen im Prüm-Netzwerk nach einem Treffer bei einer maschinellen Suche möglich.

Das Vorhaben bedroht den Bürgerrechtlern zufolge „nicht nur das Recht auf Privatsphäre und Datenschutz“. Zudem instrumentalisiere es „auch eines der Grundprinzipien der EU – die Freizügigkeit –, um die Notwendigkeit von noch mehr Polizeiarbeit zu legitimieren“. Auf Basis der Verordnung würden „die sensiblen Daten von bis zu 10% der Bevölkerung – wie DNA und Fingerabdrücke – in nationalen polizeilichen Datenbanken gesammelt“. Dazu kämen nun Gesichtsbilder. Jeder Mitgliedstaat könne diese biometrischen Daten dann automatisch abfragen.

Gemäß den Verfassern hat sich seit über 14 Jahren der Prüm-Rahmen „als untauglich erwiesen“. Untersuchungen in Slowenien etwa hätten ergeben, dass Opfer und ihre Familienangehörigen rechtswidrig in strafrechtliche Datenbanken aufgenommen wurden. Andere Beispiele zeigten, dass Unverdächtige, Freigesprochene und Zeugen in vielen EU-Staaten inklusive Deutschlands mehr oder weniger routinemäßig ohne Rechtsgrundlage in strafrechtliche Datenbanken integriert worden seien. Sicherheitsvorkehrungen seien – soweit überhaupt vorhanden – uneinheitlich. In den nationalen Datenbanken gebe es „systematische Datenschutzmängel“. Zudem stamme der Prümer Vertrag aus einer Zeit, in der die Datenschutzrichtlinie für den Justiz- und Strafverfolgungsbereich noch nicht existierte. Würden die Register der Mitgliedsstaaten nun noch weiter mit supranationalen Systemen verknüpft, multiplizierten sich die Missbrauchsrisiken.

Angesichts der mangelnden Transparenz polizeilicher Datenbanken seien sich viele Menschen nicht bewusst, dass ihre Informationen „auf unlautere und unrechtmäßige Weise verarbeitet werden“. Sie könnten daher ihre Rechte etwa auf Widerspruch oder Korrekturen nicht wahrnehmen. Die Einbeziehung ihrer Informationen in diese Datenbanken habe im schlimmsten Fall jedoch schwerwiegende Auswirkungen auf ihre Grundrechte und Freiheiten.

Das Vorhaben verschärfe das Problem einer übermäßigen polizeilichen Überwachung und das Misstrauen. Es sei „weder notwendig noch verhältnismäßig“. Die Prüm-II-Verordnung gefährde die Ansprüche auf Gerechtigkeit, Fairness und Privatheit: Chris Jones, Direktor der britischen Bürgerrechtsorganisation Statewatch, die das Papier zusammen mit anderen EDRi-Mitgliedern wie Access Now oder der Schweizer Digitalen Gesellschaft verfasst hat, meinte: „Es scheint ein Fall zu sein, in dem man versucht die Polizei zum Laufen zu bringen, wenn sie schon Probleme beim Gehen hat.“

In der Studie heißt es: „Wir erleben die zunehmende Kriminalisierung von politischer Opposition, sozialen Bewegungen, Flüchtlingen und Migranten sowie investigativen Journalisten.“ Wenn sich der Rat durchsetze, könnte die Polizei künftig „jeden als Kriminellen abstempeln.“ Solche autoritären Praktiken erlaubten es den Strafverfolgern „die Privatsphäre der Menschen ohne ausreichenden Grund oder angemessene Schutzmaßnahmen einzuschränken“. Vor allem bereits marginalisierten Gruppen drohten noch mehr Repressalien.

Die Bürgerrechtler empfehlen dem EU-Parlament, das sich zu Vorschlägen positionieren muss, die Erweiterung um Gesichtsbilder zurückzuweisen. Führerscheindaten müssten von Europol und von Drittstaaten auf jeden Fall genauso außen vor bleiben wie biometrische Merkmale. Nötig sei die Implementierung spezifischer restriktiver Vorschriften für die polizeilichen Datenbanken der Mitgliedstaaten, bevor diese an das Prüm-II-System angebunden werden. Unidentifizierte DNA-Daten und nicht stichhaltige Einträge sollten gelöscht werden. Die Abgeordneten müssten auch sicherstellen, dass Suchanfragen nur in Einzelfällen und zur Verfolgung schwerer Straftaten durchgeführt werden könnten. Zuvor hatte sich der EU-Datenschutzbeauftragte Wojciech Wiewiórowski besorgt gezeigt, dass schon der Kommissionsentwurf weit übers Ziel hinausschieße (Krempl, EU-Polizeidatenabgleich: Jeder wird verdächtig, warnen Bürgerrechtler, www.heise.de 11.09.2022, Kurzlink: https://heise.de/-7260262).

EU

Internes Dokumenten-Authentisierungssystem iFado geknackt

Unbekannte Hacker haben sich offenbar Zugang zu der europäischen Datenbank iFado (Intranet False and Authentic Documents Online) verschafft, auf die sich die Sicherheitsbehörden aller EU-Mitgliedsstaaten, Norwegens, Islands und der Schweiz bei der Bekämpfung von irregulärer Migration und organisierter Kriminalität stützen. Ein als vertraulich eingestuftes Dokument des Generalsekretariats des Europäischen Rates an die Mitgliedstaaten vom 04.07.2022 bestätigte als Nachtrag eine am 29.06.2022 verschickte Warnung, mit dem die ursprünglich bis August laufende Frist zum Zurücksetzen aller Passwörter der Nutzer drastisch verkürzt wurde: Bis 15.07.2022 mussten alle Benutzer ihre Passwörter zurücksetzen, wenn sie nicht automatisch ausgesperrt werden wollten.

Die Datenbank iFado nutzen Sicherheitsbehörden der beteiligten Staaten, um Informationen über aktuelle Sicherheitsmerkmale und Fälschungstechniken für Reisepapiere, also etwa Ausweise und Reisepässe, aber auch Führerscheine und Aufenthaltstitel zu teilen. iFado enthält die wichtigsten Informationen aus dem Fado-Datenarchiv, die bei der Kontrolle von Papieren etwa durch Polizei oder Zoll hilfreich sind. Besonders praktisch ist das für die europäische Grenzschutzagentur Frontex, so ein Sprecher: „Es sind Tausende von Dokumententypen im Umlauf. Diese alle zu kennen ist unmöglich.“ Wenn ein Mitarbeiter Zweifel an der Gültigkeit eines Dokuments habe, könne er diese mit iFado überprüfen. Die Datensammlung erleichtere insbesondere die Arbeit an EU-Grenzposten deutlich. In Deutschland haben neben den Polizeibehörden etwa auch der Zoll und Einwohnermeldeämter Zugriff auf das System, insgesamt sind es dem Bundesinnenministerium zufolge rund 1.200 Nutzende.

Personenbezogene Daten sind in der Datenbank der vom EU-Parlament beschlossenen Verordnung zufolge nur in Ausnahmefällen zu finden. Dennoch handelt es sich um höchst sensible Informationen: Durch einen Zugriff auf das System sind Unbefugte, so ein Sprecher des Bundesinnenministeriums, möglicherweise in der Lage besonders hochwertige Fälschungen zu erstellen. Es ist daher verwunderlich, dass es bislang offenbar keine Möglichkeit für teilnehmende Behörden gab Nutzerkonten mit Multi-Faktor-Authentifizierung abzusichern. Ein solches Verfahren verlangt von den Nutzern zusätzlich zum Passwort beispielsweise einen mit einer App generierten Einmalschlüssel.

In seiner Warnung verweist das zuständige Generalsekretariat des Rates auf eine laufende Ermittlung der Cybersicherheitsbehörden der EU. Das Cyber Emergency Response Team der EU hatte die Zugangsdaten für die Plattform am 22.06.2022 als Teil eines größeren Zugangsdatenpakets gefunden, das in kriminellen Foren im Darknet zum Verkauf angeboten wurde. Woher die Hacker die Daten hatten, sei bislang unklar. Auch, ob die Zugänge von den Cyberkriminellen aktiv ausgenutzt wurden, sei bislang nicht ermittelt worden, so die Warnung an die Mitgliedstaaten. Die drastisch vorgezogene Frist weist darauf hin, dass das Risiko deutlich höher als zunächst angenommen eingestuft wurde. Dass die Zugangsdaten in einem Paket angeboten wurden, könnte darauf hindeuten, dass die Hacker die Zugänge für nicht sonderlich wertvoll hielten. Es könnte aber auch sein, dass die Hacker die Zugänge bereits jahrelang genutzt hatten und nun auch noch zu Geld machen wollten. Wie die EU-Behörden den Fall tatsächlich einschätzen, blieb zunächst unklar. Weder das eigentlich zuständige Generalsekretariat des Rates noch die EU-Kommission wollten Fragen zu dem Sicherheitsvorfall beantworten.

Ende März 2020 hatte das EU-Parlament beschlossen, dass das Fado-System künftig von Frontex verwaltet werden soll. Damit soll die Plattform effizienter und sicherer betrieben werden können. So soll das System künftig verschiedene Zugriffsstufen für unterschiedliche Personengruppen zulassen. Ursprünglich sollte der Umzug auf eine neue Plattform 2023 stattfinden, aktuell scheint die EU mit 2024 zu planen (Muth, EU-Datenbank für gefälschte Ausweispapiere offenbar gehackt,

www.sueddeutsche.de 26.07.2022 = EU-Datenbank offenbar gehackt, SZ 27.07.2022, 7).

Österreich

KI anonymisiert automatisiert Gerichtsentscheidungen

In Österreich haben das Bundesministerium für Justiz (BMJ) und das Bundesrechenzentrum (BRZ) ein Verfahren entwickelt, um Gerichtsentscheidungen automatisiert zu anonymisieren. Der Einsatz von sog. künstlicher Intelligenz (KI) soll die Sachbearbeiter von repetitiven Anwendungen entlasten und einer rascheren Veröffentlichung von Gerichtsentscheidungen dienen. Für die gemeinsam entwickelte KI-Anwendung sind BMJ und BRZ am 10.10.2022 in Wien mit dem eAward in der Kategorie „Machine Learning und Künstliche Intelligenz“ ausgezeichnet worden.

Die Jury begründete ihre Entscheidung damit, dass hier KI perfekt eingesetzt werde, um repetitive Aufgaben beschleunigt abzuwickeln, was dem in der Justiz beschäftigten Personal beim Bewältigen der Arbeit helfe. Die Anwendung habe „Exportqualität in viele andere Bereiche“. Die österreichische Justizministerin Alma Zadić lobte in ihrer Stellungnahme zur Preisverleihung den Digitalisierungskurs ihres Ressorts und spricht davon, dass Österreich in dem Gebiet „eine Vorreiterrolle in Europa“ einnehme. Die Anwendung sei ein Beispiel für den verantwortungsvollen Einsatz von KI-Technologie.

Das BRZ stand dem BMJ bei der Umsetzung als technischer Partner zur Seite. Seine Aufgabe sei, „Kompetenzzentrum für die Digitalisierung in der Bundesverwaltung“ zu sein. Die Anwendung zeige das große Potenzial von Künstlicher Intelligenz und Machine Learning für den öffentlichen Sektor. Die fertige Anwendung soll, so der Geschäftsführer des BRZ, Roland Ledinger, für die Bürger einen greifbaren Mehrwert bieten. Das Bundesrechenzentrum war bei den eAwards mit mehreren Projekten für den Preis nominiert, so auch mit einem Projekt zu vertrauenswürdiger KI.

Das Rechtsinformationssystem des Bundes (RIS) veröffentlicht fast ausschließlich Entscheidungen des Obersten Gerichtshofs. Die ordentlichen Gerichte, zu denen auch etwa Landesgerichte und Oberlandesgerichte zählen, treffen in Österreich Entscheidungen, die für alle Rechtssuchenden von Bedeutung sind. Vor einer Publikation sind alle personenbezogenen Daten sowie Informationen, die Rückschluss auf die Sache und die Betroffenen zulassen, zu entfernen. Die Anonymisierung nimmt bei manueller Durchführung viel Zeit in Anspruch – mithilfe von Machine Learning und unter Einsatz von KI sei es dem BRZ gelungen den Prozess wesentlich zu beschleunigen.

Die mit dem eAward ausgezeichnete Anwendung ermöglicht es Personen, Organisationen, Orte „sowie weitere relevante Metadaten zu identifizieren, zu extrahieren und basierend auf festen Regeln zu anonymisieren“, unter Einhaltung der gesetzlichen Rahmenbedingungen. Die Anwendung soll vorhandene Registerdaten berücksichtigen und enthält offenbar eine regelbasierte Suchfunktion. Wie das Bundesrechenzentrum angibt, sind die eingesetzten Machine-Learning-Modelle auf Basis manuell markierter Gerichtsentscheidungen trainiert. Sie kommen beim Erkennen enthaltener Informationen zum Einsatz, aber auch beim Entscheiden welche Textpassagen zu anonymisieren sind. Die technische Herausforderung besteht dabei im Erkennen der unterschiedlichen Rollen der Personen im Text. So soll etwa der Name von Richterinnen und Richtern nicht anonymisiert werden, und auch die anwaltlichen Vertreter und Vertreterinnen der Streitparteien sollen im Klartext erhalten bleiben.

Andere EU-Länder sollen bereits Anfragen an die österreichische Justiz und das Bundesrechenzentrum gestellt haben. Die Anwendung und das technische Verfahren stoßen im europäischen Umfeld gemäß einem Sprecher des Bundesrechenzentrums auf erhebliches Interesse. Die Anfragen beziehen sich auf einen Know-how-Transfer, um ähnliche Anwendungen und Konzepte in anderen EU-Ländern zu implementieren. Auch in Österreich selbst sind dem Bundesrechenzentrum zufolge weitere Einsatzmöglichkeiten für die Technik vorstellbar. Der Bedarf sei auch außerhalb der ordentlichen Gerichtsbarkeit gegeben; seitens Verwaltungsgerichten und weiterer Behörden sind, so der Leitende Staatsanwalt im Justizministerium Mag. Christian Gesek, bereits Anfragen eingegangen. Ob aus Deutschland bereits Anfragen eingegangen sind, geht aus der Meldung nicht hervor.

Weitere Informationen lassen sich der Internetpräsenz des Bundesministeriums für Justiz und der Website des Bundesrechenzentrums entnehmen. Das BRZ feiert 2022 sein 25-jähriges Bestehen und ist gemäß seiner Webseite seither mit der Entwicklung sicherer IT-Lösungen befasst, „um Österreichs Public Sector fit für die Zukunft zu machen“. Als E-Government-Partner der österreichischen Verwaltung verfügt es über eines der größten Rechenzentren der Alpenrepublik (Hahn, Preis für Vorreiter: Österreich anonymisiert Justizentscheidungen mit KI-Einsatz, www.heise.de 12.10.2022, Kurzlink: https://heise.de/-7305474).

Frankreich

20-Mio.-Euro-Bußgeld gegen Clearview AI

Die französische Datenschutzbehörde Commission Nationale de l'Informatique et des Libertés (CNIL) hat gegen die US-Firma Clearview AI wegen rechtswidriger biometrischer Gesichtserkennung die Höchststrafe auf DSGVO-Basis von 20 Mio. Euro verhängt. Zuvor hat Clearview auf eine Abmahnung im Jahr 2021 hin nicht reagiert. Die Kontrolleure ordneten zudem an, dass Clearview Daten über Personen in Frankreich nicht länger erheben und verwenden darf, da es dafür keine Rechtsgrundlage gebe. Bereits gespeicherte Gesichtsbilder und zugehörige Informationen müssen laut dem Bescheid vom 17.10.2022 zudem innerhalb von zwei Monaten gelöscht werden. Die Aufsichtsbehörde verweist zur Begründung auf die „sehr ernsten Risiken für die Grundrechte der betroffenen Personen, die sich aus der von dem Unternehmen durchgeführten Verarbeitung ergeben“. Folgt Clearview der Anordnung nicht, droht der Firma

ein Zwangsgeld in Höhe von 100.000 Euro für jeden Tag der Überschreitung der Frist.

Die CNIL erhielt nach eigenen Angaben seit Mai 2020 Beschwerden einzelner Personen über die von Clearview entwickelte Gesichtserkennungssoftware. Ein Jahr später wandte sich auch die Bürgerrechtsorganisation Privacy International deswegen an sie. Bei den Untersuchungen arbeitete die Aufsichtsinstanz nach eigenen Angaben mit europäischen Kollegen zusammen: Da das Unternehmen keinen Sitz in der EU hat, seien die nationalen Behörden für Maßnahmen in ihrem eigenen Hoheitsgebiet zuständig.

Die CNIL stellte zwei Verstöße gegen die DSGVO fest: Clearview verarbeitet die sensiblen biometrischen Daten demnach unrechtmäßig, da die Firma dafür keine Einwilligung einhole und auch keine andere in Frage kommende rechtliche Basis vorliege. Zudem berücksichtige das Unternehmen Rechte der Betroffenen etwa auf Einsicht und zum Löschen ihrer Daten nicht zufriedenstellend und effizient. Das Unternehmen extrahiere Fotos aus einer Vielzahl von Webseiten, sozialen Netzwerken und Videos. Auf diese Weise habe es sich weltweit mittlerweile über 20 Milliarden Bilder angeeignet. Mithilfe dieser Sammlung vermarkte es den Zugang zu seiner Bilddatenbank vor allem an Strafverfolger in Form einer App, in der eine Person mithilfe eines Fotos gesucht werden könne. Die Betroffenen rechneten realistischerweise aber nicht damit, dass ihre Bilder in ein Gesichtserkennungssystem eingespeist werden, „das von Staaten für polizeiliche Zwecke genutzt werden kann“.

Nach der Verfügung von November 2021 hatte Clearview zwei Monate Zeit, um die Anordnung zum Stopp des Sammelns und Nutzens von Daten französischer Staatsbürger zu befolgen und dies gegenüber der Aufsichtsbehörde nachzuweisen. Das Unternehmen reagierte jedoch nicht. Das angekündigte Sanktionsverfahren nahm so seinen Lauf.

Während des gesamten Verfahrens hatte gemäß der CNIL Clearview nicht in angemessener Form mit ihnen zusammengearbeitet. So habe das Unternehmen das ihm zugesandte Untersuchungsformular nur sehr unvollständig beantwortet und die spätere förmliche Aufforderung völlig missachtet. Der Sanktionsausschuss berücksichtigte bei der Strafe daher auch einen Verstoß gegen die Pflicht nach der DSGVO, mit der Aufsicht zu kooperieren.

In Europa verhängte auch die britische Datenschutzbehörde ICO im Mai 2022 eine Strafe in Höhe von rund 8,9 Millionen Euro gegen Clearview. Angekündigt hatte sie zunächst ebenfalls rund 20 Millionen Euro, berücksichtigte dann aber doch mildernde Umstände. Der frühere Hamburgische Datenschutzbeauftragte Johannes Caspar ging ebenfalls bereits gegen die Firma vor. Kanadische Behörden haben Clearview untersagt den Dienst in mehreren Provinzen weiter anzubieten. Das Unternehmen muss zudem alle Bilder und zugehörigen Daten der dortigen Einwohner löschen. Es peilt trotzdem an seine Speicher mit 100 Milliarden Gesichtsfotos zu füllen (Krempl, DSGVO-Bußgeld: Frankreichs Datenschützer fordern 20 Millionen Euro von Clearview, www.heise.de 21.10.2022, Kurzlink: https://heise.de/-7315416).

Griechenland

Geheimdienst hörte Politiker und Journalisten ab

Am 05.08.2022 wurde bekannt, worüber zunächst spekuliert worden war, nämlich dass der griechische Geheimdienst EYP den Europaabgeordneten und Chef der zweitgrößten Oppositionspartei Pasok, Nikos Androulakis, und den Finanzjournalisten Thanasis Koukakis monatelang abgehört hat. Regierungschef Kyriakos Mitsotakis, dem der Geheimdienst direkt unterstellt ist, erklärte: „Ich wusste nichts davon, und natürlich hätte ich das nie genehmigt.“ EYP-Chef Panagiotis Kontoleon und der für den Geheimdienst zuständige Generalsekretär im Amt des Ministerpräsidenten, Grigoris Dimitriadis, ein Neffe und langjähriger Vertrauter des Premiers, mussten umgehend ihre Ämter aufgeben. Premierminister Mitsotakis meinte, das Ganze sei ein Fehler gewesen, „legal“ zwar, weil von einem Staatsanwalt angeordnet, aber „politisch inakzeptabel“. Er gab sich in seiner öffentlichen Ansprache zum Skandal zerknirscht und kündigte Reformen an, die den Geheimdienst stärkerer Kontrolle und Transparenz unterwerfen sollen.

Selbst regierungsfreundliche Zeitungen schrieben von „der ernstesten Regierungskrise“ seit Mitsotakis’ Amtsantritt vor drei Jahren. Die linksgerichtete Oppositionspartei Syriza sprach von einem „griechischen Watergate“, für das Mitsotakis die Verantwortung trage und forderte deshalb den Rücktritt des Premiers. Syriza-Chef Alexis Tsipras verwies darauf, dass Mitsotakis gleich nach seinem Amtsantritt im Sommer 2019 mit einer Gesetzesänderung den Geheimdienst sich selbst direkt unterstellt hatte. Tsipras fordert nun Auskunft darüber, welche weiteren Politiker und Journalisten bespitzelt werden.

Der Europaabgeordnete Androulakis hatte von einem Sicherheitsdienst des Europäischen Parlaments erfahren, dass es Versuche gegeben habe sein Smartphone mit einer Spionage-Software namens Predator zu infizieren, die unter anderem Passwörter und den Browser-Verlauf ausspähen kann sowie Zugriff auf Kamera und Mikrofon ermöglicht. Am 04.08.2022 war Geheimdienstchef Kontoleon zur Berichterstattung ins Amt des Ministerpräsidenten einbestellt worden. Dort soll er erklärt haben, Androulakis sei auf Wunsch der Geheimdienste der Ukraine und Armeniens abgehört worden. Die ausländischen Dienste hätten sich für Androulakis’ Rolle in einem Ausschuss des Europäischen Parlaments, der sich mit den EU-Handelsziehungen zu China befasste, interessiert. Die Botschaften der Ukraine und Armeniens in Athen dementierten die Meldungen vehement. Den Abhörantrag genehmigte im September 2021 die zuständige Staatsanwältin Vasiliki Vlachou. Mehrere Regierungsvertreter hatten Androulakis persönliche Gespräche über die Vorgänge angeboten; dies lehnte er ab und forderte stattdessen, es müsse alles öffentlich gemacht werden, etwa über einen parlamentarischen Untersuchungsausschuss.

Unklar blieb, warum und auf wessen Initiative der Finanzjournalist Koukakis abgehört wurde. Die Organisation United Reporters berichtet von einem

Dokument, aus dem hervorgehen soll, der Geheimdienst EYP habe Koukakis „aus Gründen der nationalen Sicherheit“ belauscht. Seine Bespitzelung könnte damit zu tun haben, dass er Korruptionsfälle in Politik und Wirtschaft sowie angebliche Fälle von Geldwäsche im Bankenwesen recherchierte. Sein Handy war am 21.07.2021 mit der Spionagesoftware Predator infiziert worden. Die Regierung bestritt damals jede Beteiligung.

Koukakis beantragte bei der zuständigen Aufsichtsbehörde ADAE Auskunft, ob er abgehört werde. Noch während er auf eine Antwort wartete, brachte die Regierung eine Gesetzesänderung durchs Parlament, die es der Behörde untersagt Betroffenen Auskunft über Abhörpraktiken zu geben. Die griechische Regierung bestritt öffentlich Predator angeschafft zu haben.

Die Vorwürfe, Athen schränke die freie Berichterstattung im Land massiv ein, verstärken sich. Im April 2022 äußerten das Internationale Presse-Institut (IPI) und weitere der Pressefreiheit verpflichtete Organisationen in einem Brief an Ministerpräsident Mitsotakis „ernste Besorgnisse“ wegen der Bespitzelung von Journalisten in Griechenland. In der jährlichen Weltrangliste der Pressefreiheit der Organisation Reporter ohne Grenzen ist Griechenland inzwischen auf Rang 108 von 180 abgerutscht. Kein Land der Europäischen Union steht weiter unten auf der Liste.

Die griechische Staatspräsidentin Katerina Sakellaropoulou, eine hoch angesehene Juristin, schaltete sich auch in die Debatte ein. Das Recht auf Privatsphäre sei ein Fundament einer demokratischen und liberalen Gesellschaft, sagte sie und forderte eine „sofortige und vollständige Aufklärung“ der Abhör-Affäre. Eine Sprecherin der EU-Kommission erklärte mit Blick auf die Vorgänge in Griechenland, die Mitgliedsstaaten müssten „ihre Sicherheitsdienste kontrollieren und sicherstellen, dass sie die Grundrechte vollumfänglich respektieren“ (Höhler, Eine Abhöraffäre bringt den griechischen Premier Mitsotakis in Bedrängnis, www.handelsblatt.com 07.08.2022; Zick, Spitzelaffäre setzt Mitsotakis zu, SZ 13.-15.08.2022, 9).

EU/Irland

Hohes Bußgeld gegen Meta wegen Instagram

Die irische Datenschutzbehörde DPC fordert vom US-amerikanischen Konzern Meta wegen Datenschutzverstößen seiner Tochterfirma Instagram mit Bescheid vom 02.09.2022 ein Bußgeld in Höhe von 405 Millionen Euro. Die DPC hatte eine erste Überprüfung der Vorwürfe gegen das soziale Netzwerk Instagram im September 2020 gestartet. Dabei geht es um die Verarbeitung von Daten Minderjähriger. Im Dezember 2021 leitete die Behörde dann ein formelles Verfahren nach Artikel 60 DSGVO ein.

Instagram wird vorgeworfen jugendlichen Nutzern im Alter von 13 bis 17 Jahren erlaubt zu haben Geschäftskonten auf der Plattform einzurichten. Die Jugendlichen seien auf solche Konten gewechselt, um mehr Daten zu Interaktionen ihrer Beiträge einsehen zu können. Zuvor habe Instagram diese Funktionen bei Privatkonten in einigen Ländern deaktiviert. Durch den Wechsel auf Geschäftskonten seien die Kontaktinformationen der Jugendlichen öffentlich zugänglich gewesen.

Meta erklärte, dass inzwischen alle Nutzer unter 18 Jahren ihr Konto automatisch auf „privat“ gestellt haben, wenn sie sich bei Instagram anmeldeten. Dadurch könnten auch Erwachsene keine Nachrichten an Jugendliche schicken, die ihnen nicht folgten. Das Unternehmen teilte zudem mit, dass „wir nicht damit einverstanden sind, wie diese Geldstrafe berechnet wurde und beabsichtigen dagegen Berufung einzulegen“.

Die Geldbuße gegen Instagram ist eine der höchsten, die bislang auf Basis der DSGVO verhängt wurden. Sie übertrifft die Summe von 225 Millionen Euro, die Whatsapp zahlen sollte (DANA 4/2021, 253). Die Luxemburger Datenschutzbehörde CNPD verhängte gegen den Versandhändler Amazon eine Strafe in Höhe von 746 Millionen Euro (DANA 4/2021, 252), gegen die das Unternehmen bereits erfolgreich Widerspruch einlegte (Greis, Instagram soll 405 Millionen Euro Bußgeld zahlen, www.golem.de 06.09.2022).

Großbritannien

Straffällige Asylsuchende werden mit GPS und Biometrie überwacht

Migranten, die wegen einer Straftat verurteilt wurden, sollen nach Plänen der britischen Ministerien für Inneres und Justiz mit einer Smartwatch mit biometrischer Gesichtserkennung und GPS-Tracking überwacht werden. Das Verfahren ersetzt elektronische Fußfesseln, indem es per GPS Standortdaten erfasst und die Betroffenen zusätzlich mithilfe der automatisierten Biometrie kontrolliert. Bis zu fünf Mal am Tag soll ein Gesichtsscan durchgeführt werden. Im Mai 2022 beauftragte die britische Regierung gemäß einem auf Dokumenten basierenden Pressebericht die Technologiefirma Buddi mit der Lieferung von „nicht fest montierten Geräten“ zur Überwachung „bestimmter Personengruppen“ im Rahmen des Satellitenverfolgungsdienstes des Innenministeriums. Das System soll dann im Herbst in ganz Großbritannien eingeführt werden und zunächst ca. 6 Mio. britische Pfund kosten.

Der Vertrag mit dem Lieferanten, der bislang vor allem für den Vertrieb von Smartwatches mit Hausnotruffunktion bekannt ist, wurde vom Justizressort veröffentlicht. In den Unterlagen findet sich kein Hinweis darauf, ob die Regierung Risikobewertungen durchführen ließ, die abwägen, ob es angemessen ist straffällige Asylbewerber mit den vorgesehenen Mitteln zu überwachen. Gemäß einem Papier vom August 2021, das die Datenschutzorganisation Privacy International (PI) auf Basis des britischen Informationsfreiheitsgesetzes erlangt hat, führte das Innenministerium Datenschutz-Folgenabschätzungen für die Technik allgemein durch, bevor die Wahl auf einen konkreten Anbieter fällt. Das System soll gemäß den Dokumenten eine „tägliche Überwachung von Personen“ ermöglichen, „die einer Einwanderungskontrolle unterliegen“. Voraussetzung ist demnach die Auflage jederzeit eine Fußfessel oder eine Smartwatch tragen zu müssen. Das Innenressort beteuert, dass nur verurteilte Straftäter erfasst würden, nicht Asylbewerber generell.

Zusammen mit den Gesichtsfotos sollen den Unterlagen zufolge Informationen wie Name, Geburtsdatum und Nationalität bis zu sechs Jahre lang gespeichert werden. Dazu kommen planmäßig Bewegungsprofile: Die Standorte der Verpflichteten sollen „rund um die Uhr verfolgt" werden, „sodass Daten zur Überwachung von Wegen aufgezeichnet werden können". Die mit den vernetzten Uhren aufgenommenen Fotos würden dann mit den biometrischen Gesichtsbildern in einschlägigen Datenbanken des Innenministeriums abgeglichen. Schlage die automatisierte Bildüberprüfung fehl, müsse eine händische Kontrolle durchgeführt werden. Die Daten sollen mit den beiden beteiligten Ministerien und der Polizei geteilt werden, wobei letzteres prinzipiell keinen neuen Ansatz darstelle. Auch von Ausgangssperren und Verbotszonen ist die Rede.

In einem Bericht des Rechnungshofs vom Juni 2022 erklärte die Regierung, dass sie „die elektronische Überwachung als kosteneffiziente Alternative zur Inhaftierung ansieht". Die Maßnahme trage zu „den Zielen des Schutzes der Öffentlichkeit und der Verringerung der Rückfälligkeit bei". Den Kassenprüfern zufolge war zunächst geplant die Smartwatches von der Firma G4S zu beziehen, die auch für die elektronischen Fußfesseln zuständig ist. Das Justizministerium hatte bei diesen Geräten aber Schwächen bei der Cybersicherheit moniert.

PI-Aktivisten warnten in einer Eingabe an die Regierung im Mai 2022: „Die grundlegenden Veränderungen, die sich durch die Einführung von GPS-Geräten ergeben haben, können gar nicht hoch genug eingeschätzt werden. Sie ermöglichen die Überwachung des Standorts einer Person rund um die Uhr sowie die Live-Verfolgung". Dies bedeute, dass sich die Bewegungen einer Person in Echtzeit verfolgen ließen. Der geplante Ansatz gehe über die bloße elektronische Überwachung von Kautionsverletzungen im gesetzlich zulässigen Rahmen weit hinaus. Die Batterielaufzeit der Fußfesseln sei zudem mangelhaft.

Privacy International hat eine Kampagne gestartet, um das GPS-Tracking von Menschen mit Migrationshintergrund zu stoppen. Dazu die PI-Rechtsexpertin Lucie Audibert: „Gesichtserkennung ist bekanntermaßen eine unvollkommene und gefährliche Technologie, die dazu neigt farbige Menschen und Randgruppen zu diskriminieren." Die eingesetzten Algorithmen seien höchst fehleranfällig. Kein anderes Land in Europa setze „diese entmenschlichende" und tief in die Grundrechte einschneidende Technik gegen Migranten ein. Die Londoner Strafrechtlerin Monish Bhatia warnte, dass derart elektronisch Überwachte teils „Symptome von Angstzuständen, Depressionen, Selbstmordgedanken" entwickelten. Ihre psychische Gesundheit könne sich allgemein verschlechtern (Krempl, Gesichtserkennung: London will straffällige Migranten per Smartwatch überwachen, www.heise.de 06.08.2022, Kurzlink: https://heise.de/-7205172).

Ukraine

Schwarze Liste und Meinungsfreiheit

Die „Emma"-Herausgeberin Alice Schwarzer und der SPD-Fraktionsvorsitzende im Deutschen Bundestag Rolf Mützenich wurden Ende Juli 2022 von der ukrainischen Regierung auf eine internationale Schwarze Liste mit 75 Personen gesetzt, die „Erzählungen fördern, die mit der russischen Propaganda übereinstimmen". Die ukrainische Botschaft in Berlin bestätigte die Echtheit der Liste. Neben den beiden prominentesten Mitgliedern finden sich dort auch der Politikwissenschaftler Prof. Johannes Varwick und die EAP-Sektenführerin, Antisemitin und Rechtsextremistin Helga Zepp-Larouche. Das „Zentrum zur Bekämpfung von Desinformation" beim Nationalen Sicherheitsrat der Ukraine erklärte, „das Zentrum prüfe sehr sorgfältig, wer die Kriterien erfülle, um auf diese Liste zu gelangen" (Appel, https://extradienst.net/2022/07/30/gedankenfreiheit-im-krieg/).

USA

Kindesmissbrauchsbekämpfung behindert ärztliche Kinderbehandlung

Während in der Europäischen Union lautstark über Pläne für eine Chatkontrolle zum Kampf gegen Kindesmissbrauch diskutiert wird (DANA 2/2022, 100 f.; s.o. S. 252), zeigen zwei Fälle aus den USA, welche unvorhergesehenen Konsequenzen solche Verfahren haben können. Gemäß einem Medienbericht haben besorgte Eltern Fotos des Genitalbereichs ihres Kindes an Ärzte geschickt und daraufhin den Zugang zu allen genutzten Google-Diensten verloren. Obwohl die Strafverfolgungsbehörden in beiden Fällen die Ermittlungen eingestellt hätten, blieben die Google-Dienste für beide gesperrt. Einer der Väter erwartet nichts mehr von dem IT-Konzern, sondern hofft, dass er die gespeicherten Daten zumindest von der Polizei zurückbekommen kann.

In beiden Fällen ging es um Fotos, die auf eine ärztliche Anfrage hin gemacht und versendet wurden. Dabei sei es, so der Bericht, darum gegangen, schon vor dem Besuch beim Arzt einen Eindruck von Erkrankungen im Genitalbereich der kleinen Jungen zu erhalten. Auf den Android-Smartphones, bei denen die gemachten Fotos automatisch mit Google synchronisiert und in die Cloud geladen wurden, führte spezielle Software von Google nicht nur einen Abgleich mit bekannten Darstellungen von Kindesmissbrauch durch, sondern suchte automatisch nach neuen und gab dann eine Warnung aus. Daraufhin sei es zu einer ausführlicheren Analyse, Mitteilungen an Strafverfolger und die Sperrung aller genutzten Dienste gekommen.

In einem Fall verlor der Vater nicht nur den Zugriff auf seinen Mail-Account und sein komplettes Adressbuch, sondern auch alle Fotos, mit denen er das erste Lebensjahr seines Sohnes dokumentiert hatte. Weil er auch seinen Handyvertrag über Google abgeschlossen hatte, musste er sich nicht nur einen neuen zulegen. Ohne den Zugang zu seiner alten Handynummer konnte er sich auch nicht mehr in andere Internetdienste einloggen. Alles in allem wurde er, so der Bericht, von einem Großteil seines digitalen Lebens ausgesperrt. Der zweite Vater sei gerade dabei gewesen, ein Haus zu kaufen. Als sein Gmail-Account gesperrt worden sei, habe das zu Problemen mit dem Makler geführt.

Angesichts dessen erneuerte Jon Callas von der Bürgerrechtsorganisation Electronic Frontier Foundation deren

Kritik an der automatischen Durchleuchtung privater Daten: „Das ist genau das Albtraum-Szenario, vor dem wir uns alle Sorgen machen.“ Zwar wurde bei beiden Vätern nach Ermittlungen von der Polizei bestätigt, dass es keine Vorwürfe gegen sie gibt, aber den Zugriff auf ihre Google-Accounts haben sie nicht wieder. Auch auf Nachfrage habe der Konzern bestätigt, dass man dabei bleibe. Eine Jura-Professorin, die sich mit der Materie beschäftigt, spekulierte, dass es aus der Perspektive des Konzerns einfacher sei so zu verfahren als selbst entscheiden zu müssen, was akzeptabel sei und was nicht. Einer der betroffenen Väter benutzt nun einen E-Mail-Account von Hotmail, wofür er von Leuten verspottet werde (Holland, Missbrauchsverdacht: Intime Fotos vom Kind für den Arzt-Google-Dienste gesperrt, www.heise.de 22.08.2022, Kurzlink: https://heise.de/-7238900).

USA

Twitter-Mitarbeiter von Geheimdiensten fremder Staaten

Peiter Zatko, der ehemalige Sicherheitschef des US-Konzerns Twitter, behauptete bei einer Anhörung vor dem Justizausschuss des US-Senats, dass die dortigen Sicherheitsmängel so schwerwiegend sind, dass sie eine Gefahr für die Nationale Sicherheit der USA und mutmaßlich auch anderer Staaten darstellen. Während seiner Zeit bei Twitter habe die US-Bundespolizei das Unternehmen informiert, dass dort mindestens ein Mitarbeiter des chinesischen Ministeriums für Staatssicherheit angestellt sei. In einem Gespräch über solch einen möglichen Agenten habe er von einer Führungsperson bei Twitter gehört: „wenn wir schon einen haben, was macht es aus, wenn es mehr sind.“

Zatko hatte Twitter Anfang 2022 verlassen und im Sommer eine Whistleblower-Beschwerde gegen seinen ehemaligen Arbeitgeber bei verschiedenen US-Institutionen eingereicht. Vor den US-Abgeordneten sagte er nun, dass er bei seinem Einstieg festgestellt habe, dass das Unternehmen 10 Jahre überfällige kritische Sicherheitslücken angesammelt habe. Bei deren Abarbeitung seien keine nennenswerten Fortschritte erzielt worden: „Das war eine tickende Zeitbombe.“ Er habe das wiederholt der Führungsebene des Unternehmens mitgeteilt und erst nachdem seine Warnungen unbeachtet geblieben seien, habe er sich an die Behörden gewandt.

Weil Ingenieure und Ingenieurinnen bei Twitter nicht in Testumgebungen arbeiteten, sondern an Twitter selbst, hätten ausländische Geheimdienstler Zugang zu allen Daten. Angesichts dessen sowie der Zustände bei dem Unternehmen insgesamt mache ein Geheimdienst, der das nicht ausnutze und niemanden dort platziere, „höchstwahrscheinlich seinen Job nicht richtig“. Vor seiner Behauptung, dass Twitter von einem chinesischen Agenten gewusst habe, hatte Zatko bereits behauptet, dass Indien den Konzern dazu verpflichtet habe einen Agenten anzustellen. Auch Spione Saudi-Arabiens waren bereits bei Twitter entdeckt worden.

Vor der Anhörung hatten die beiden Vorsitzenden des Justizausschusses an Twitter-Chef Parag Agrawal geschrieben und von „schweren Bedenken“ gesprochen, die die Anschuldigungen auslösen würden. Twitter spiele eine bedeutende Rolle in der Kommunikation der Vereinigten Staaten und sei weltweit wichtig. Von Agrawal wollen sie angesichts der jüngsten Enthüllungen wissen, was sein Unternehmen unternehme, um Daten vor Geheimdiensten zu schützen, die Twitter infiltriert hätten. Außerdem soll er erläutern, wie Nutzerdaten vor unbefugten Zugriffen insgesamt geschützt würden. Mit Charles Grassley meinte der führende Republikaner in dem Gremium, dass er sich nicht vorstellen könne, dass Agrawal angesichts der Vorwürfe seinen Posten behalten kann.

Zatko (Aliasname „Mudge“) erklärte zudem, dass Twitter den Aufsichtsrat und die Investoren in die Irre geführt habe. Der laxe Umgang mit den Nutzerdaten stelle eine reale Gefahr für Millionen Amerikaner und Amerikanerinnen dar, sowie für die Demokratie in den USA. Seine Aussagen haben angesichts der Auseinandersetzung um die Übernahmepläne von Twitter durch Elon Musk besondere Brisanz. Der Chef von Tesla und SpaceX weigerte sich, die Kaufvereinbarung wegen angeblicher Falschangaben und Vertragsbrüche des Unternehmens einzuhalten. Die Äußerungen Zatkos erfolgten am 13.09.2022 und damit am gleichen Tag, an dem die Aktionäre Twitters die geplante Übernahme durch Elon Musk genehmigten (Holland, Twitter-Whistleblower: Auch China und Indien haben Agenten eingeschleust, www.heise.de 14.09.2022, Kurzlink: https://heise.de/-7263041).

USA

FTC geht wegen Auswertung von Standortdaten vor

Die US-Wettbewerbs- und Verbraucherschutzbehörde Federal Trade Commission (FTC) verklagt den Datenbroker Kochava, weil er sensible Standortdaten verkauft haben soll, mit denen bestimmte Abtreibungswillige, religiöse Gläubige oder andere Personen identifiziert werden können, die möglicherweise von Diskriminierung, Einschüchterung oder sogar Gewalt bedroht sind.

In der am 29.08.2022 eingereichten Klage wird dem App-Analyseunternehmen Kochava vorgeworfen bei den Standortdaten, die zum großen Teil ohne Wissen der Besitzer von Handys gesammelt werden, grundlegende Datenschutzbestimmungen nicht eingehalten zu haben, so die FTC: „Die Daten von Kochava können Aufschluss über die Besuche von Menschen in Kliniken für reproduktive Gesundheit, Gotteshäusern, Obdachlosenheimen, Einrichtungen für häusliche Gewalt und Suchtkrankenhäusern geben. Durch den Verkauf von Tracking-Daten ermöglicht es Kochava anderen Personen zu identifizieren und sie der Gefahr von Stigmatisierung, Stalking, Diskriminierung, Arbeitsplatzverlust und sogar physischer Gewalt auszusetzen.“ Kochava wird von der FTC aufgefordert den Verkauf sensibler Daten einzustellen und alle gesammelten Informationen zu löschen. Kochava ist ein Unternehmen für Marketingdaten, das große Marken wie Disney, McDonald's und Hilton zu seinen Kunden zählt.

Die Klage folgt auf eine Zusage der FTC gegen die Weitergabe von medizinischen Standortdaten vorzugehen.

Das ist ein weit verbreitetes Problem, das in der Abtreibungsdebatte in den USA besonders brisant geworden ist. Nach der Entscheidung des Obersten Gerichtshofs, der in diesem Jahr das Recht auf Abtreibung auf Bundesebene aufhob, hat die FTC signalisiert, dass sie sich zunehmend auf den Schutz gesundheitsbezogener Daten konzentrieren wird. Abtreibungsgegner in den USA sammeln bereits Daten vor Kliniken für die Strafverfolgung. So werden Körperkameras und Nummernschildverfolgung eingesetzt, um Menschen nachzuspüren, die zu Abtreibungskliniken kommen (DANA 3/2022, 194 ff.).

US-Bürgerrechtsorganisationen sorgen sich nach dem Urteil zur Abtreibung um den Datenschutz. Sie warnen davor, dass neue bundesstaatliche Gesetze in den USA, die Abtreibungen einschränken, dazu führen könnten, dass die Standortdaten von Abtreibungswilligen als Beweis für Fehlverhalten gegen sie verwendet werden. So wächst die Sorge, dass der digitale Fingerabdruck einer Person – einschließlich besuchter Websites, Standortdaten eines Telefons oder privater Nachrichten auf einer sozialen Plattform – künftig verwendet werden könnte, um ein Strafverfahren gegen jemanden zu führen, der eine Abtreibung durchgeführt hat. Die Tech-Branche schweigt zur Datenschutzproblematik weitestgehend.

Auf Druck der demokratischen Senatorin Elizabeth Warren und anderen verpflichteten sich die Datenbroker SafeGraph und Placer.ai Geolokalisierungsdaten in der Umgebung von Kliniken für reproduktive Gesundheit nicht mehr zu verkaufen. Google erklärte kürzlich, dass es Standortdaten nach Besuch von Abtreibungskliniken löschen wird. Der FTC zufolge waren die Daten von Kochava nicht anonymisiert, so dass es durch die Kombination der Standortdaten mit Daten aus anderen Quellen möglich war die tatsächliche Identität einer Person anhand der von Kochava angebotenen Informationen zu ermitteln. Bei der Untersuchung, die zu der Klage führte, analysierte die FTC nach eigenen Angaben eine Stichprobe von Kochava, die mehr als 60 Millionen einzelne Mobilgeräte innerhalb einer einzigen Woche umfasste. Die Daten von Kochava enthalten demnach genaue, mit einem Zeitstempel versehene Breiten- und Längengradinformationen für einzelne Verbraucher, heißt es in der Klage.

Dieser zufolge konnte die FTC anhand einer kostenlosen Kochava-Datenstichprobe ein mobiles Gerät identifizieren, das eine Klinik für reproduktive Gesundheit von Frauen besucht hat, und es dann mit einer Privatadresse in Verbindung bringen, die wahrscheinlich die Identität des Nutzers oder der Nutzerin preisgeben würde. Die FTC fordert Kochava auf Sicherheitsvorkehrungen an sensiblen Orten zu treffen, was zu „vernünftigen“ Kosten möglich wäre (Knobloch, US-Wettbewerbshüter verklagen Datenmakler wegen Tracking von Klinikbesuchern, www.heise.de 29.08.2022, Kurzlink: https://heise.de/-7247692).

USA

Digitale Kfz-Kennzeichen in Kalifornien

Ende September 2022 unterzeichnete der Gouverneur von Kalifornien, Gavin Newsom, eine Gesetzesvorlage, die digitale Nummernschilder, die neben dem Kennzeichen auch andere Informationen anzeigen können, für alle Fahrzeuge in dem US-Bundesstaat erlaubt. Damit werden die E-Ink-Kennzeichen zu einer legalen Alternative zum herkömmlichen Metallschild. Dem Gesetz war ein erfolgreiches Pilotprogramm aus dem Jahr 2018 vorausgegangen. Das überarbeitete Gesetz, so die kalifornische Abgeordnete Lori Wilson, die den Gesetzentwurf mitverfasst hat, „schafft das notwendige Gleichgewicht zwischen Innovation und Datenschutz und digitalisiert gleichzeitig das Einzige, was an unseren Autos heute noch veraltet ist: die Nummernschilder“.

Bisher gibt es mit Reviver nur einen einzigen zugelassenen Hersteller von digitalen Nummernschildern. Das Produkt des Unternehmens mit dem Namen RPlate verwendet einen monochromen E-Ink-Bildschirm, der durch eine Linse oder Abdeckung geschützt ist, die laut Reviver „sechsmal stärker als Glas“ ist. Das Schild verfügt außerdem über Bluetooth Low Energy und LTE „für stromsparendes IoT“ und wird von einer mehrere Jahre haltbaren Batterie betrieben. Das RPlate zeigt das Nummernschild des Fahrzeugs an, kann aber über eine Smartphone-App auch andere Meldungen anzeigen, z.B. dass das Fahrzeug gestohlen wurde.

Das von Ars Technica im Rahmen des Pilotprojekts getestete digitale RPlate-Kennzeichen kostet, so deren Bericht, 700 US-Dollar plus einer Servicegebühr von 7 US-Dollar pro Monat. Künftig werde es ein Abonnementmodell geben, das für ein Privatfahrzeug 19,95 US-Dollar pro Monat für 48 Monate oder 215,40 US-Dollar pro Jahr für vier Jahre kostet. Es gibt auch eine kabelgebundene Version für Flottenkunden und Nutzfahrzeuge, bei der Bluetooth und die Batterie wegfallen, dafür aber GPS und Hintergrundbeleuchtung hinzukommen. Sie ist mit 24,95 US-Dollar monatlich für 48 Monate oder 275,40 US-Dollar jährlich für vier Jahre etwas teurer.

Wegen möglicher Auswirkungen auf die Privatsphäre verbietet das kalifornische Gesetz generell die Ausstattung eines digitalen Kennzeichens mit GPS; Flotten und Nutzfahrzeuge sind von dieser Anforderung allerdings ausgenommen. Das Verändern, Fälschen, Nachahmen oder sonstige Hacken von Nummernschildern macht das neue Gesetz zu einer Straftat.

Arbeitgeber dürfen digitale Nummernschilder nicht verwenden, um ihre Angestellten zu verfolgen oder zu überwachen. Doch, so Ars Technica, „der Gesetzentwurf erlaubt es einem Arbeitgeber, ein alternatives Gerät zu verwenden, um einen Angestellten während der Arbeitszeit zu orten, zu verfolgen, zu beobachten, abzuhören oder anderweitig zu überwachen, wenn dies für die Erfüllung der Pflichten des Angestellten unbedingt erforderlich ist“. Flotten, die sich frühzeitig für digitale Nummernschilder entscheiden, würden mit ziemlicher Sicherheit eine Flottenmanagementplattform verwenden, die bereits das Verhalten und den Standort ihrer Fahrer während der Arbeit überwacht (Knobloch, Kalifornien: Digitale Nummernschilder für alle Fahrzeuge zugelassen, www.heise.de 13.10.2022. Kurzlink: https://heise.de/-7308209).

Mexiko

Pegasus gegen Menschenrechtler

In der laufenden Amtszeit des linken Präsidenten von Mexiko, Andrés Manuel López Obrador (2019-2021), wurde von der Armee offenbar die israelische Spionagesoftware Pegasus gegen Journalisten, Menschenrechtsaktivisten und zivile Organisationen eingesetzt. Diese haben am 03.10.2022 angekündigt Strafanzeige gegen das mexikanische Verteidigungsministerium (Sedena) zu stellen. Ein Tag zuvor wurde der Fall in einem Investigativartikel enthüllt.

Der von dem Onlineportal Animal Político, der Zeitschrift Proceso, dem Nachrichtenportal Aristegui Noticias und dem Netzwerk zur Verteidigung digitaler Rechte (Red en Defensa de los Derechos Digitales - R3D) veröffentlichte Bericht beschreibt, wie die mexikanische Armee die Pegasus-Spyware der israelischen Firma NSO Group im Jahr 2019 gekauft hat, um Aktivisten und Journalisten auszuspionieren. Schon die Vorgängerregierung von Enrique Peña Nieto (2012-2018) hatte dem Bericht zufolge mit Hilfe von Pegasus Journalisten und Menschenrechtsaktivisten ausspioniert.

Mindestens ein Aktivist und zwei Journalisten haben auf ihren Telefonen Beweise für die Überwachung ihrer persönlichen Daten durch die Streitkräfte gefunden. Dabei wurden Informationen über Textnachrichten, Anrufe, E-Mails, Messaging-Anwendungen, Kontaktbücher, Notizen, Fotos und alle auf den Geräten gespeicherten Dateien mit der Software ausspioniert. Die Mobiltelefone der Opfer können vollständig überwacht werden, da die Software Zugriff auf alle Informationen des Geräts ermöglicht, auch auf die verschlüsselten. Gemäß der Untersuchung hat Sedena im Juni 2019, also mehr als sechs Monate nach dem Amtsantritt von López Obrador, das Unternehmen Comercializadora Antsua unter Vertrag genommen, die mexikanische Vertretung der israelischen NSO Group, die die Pegasus-Malware vertreibt. Der Vertrag wurde in E-Mails der Armee bestätigt, die von der Gruppe Guacamaya nach einem Hackerangriff veröffentlicht wurden.

Das Citizen Lab der Universität Toronto stellte fest, dass die Telefone des Menschenrechtsaktivisten Raymundo Ramos, des Journalisten Ricardo Raphael und eines Journalisten von Animal Politico, der nicht genannt werden möchte, im Jahr 2019 mit der Malware infiziert wurden. Alle drei hatten gemeinsam, dass sie Fragen im Zusammenhang mit Menschenrechtsverletzungen durch die Streitkräfte untersuchten.

Nachdem schon 2017 während der Amtszeit von Peña Nieto Pegasus in Mexiko eingesetzt worden war, behauptete im Jahr 2019 der neue Präsident López Obrador, dass die Regierung seit Beginn seiner Amtszeit keine Spyware wie Pegasus mehr verwende: „Wir haben Anweisungen gegeben, dass es keine Spionage geben wird.“ Ricardo Raphael, einer der drei Betroffenen, ist der Ansicht, dass die dokumentierten Fakten darauf hindeuten, dass der Geheimdienstapparat des Landes vom Militär dominiert wird: „Dies zeigt, dass die Bundesregierung ihre Zusage, die illegale Spionage in Mexiko zu beenden, nicht eingehalten hat.“

Zahlreiche weitere Länder, u.a. Saudi-Arabien, Marokko oder die Vereinigten Arabischen Emirate, nutzten die Pegasus-Software zur politischen Überwachung. Zuletzt war eine großangelegte Überwachungskampagne in Thailand aufgedeckt worden. Die Organisation Forensic Architecture dokumentiert auf einer interaktiven Plattform über 60 Fälle, in denen mit einer NSO-Spyware Aktivisten ausgespäht wurden und „wie die NSO Group Staatsterror ermöglicht“. Apple hat laut eigenen Angaben inzwischen Warnmeldungen an potenziell betroffene Nutzerinnern und Nutzer in 150 Ländern weltweit verschickt. Im Mai 2022 nahm der Untersuchungsausschuss des EU-Parlaments zum Einsatz von Pegasus und vergleichbarer Spionagesoftware mit einer Anhörung von IT-Sicherheitsexperten seine inhaltliche Arbeit auf (Knobloch, Spionagesoftware Pegasus sorgt in Mexiko erneut für Ärger, www.heise.de 04.10.2022, Kurzlink: https://heise.de/-7282937; vgl. u.a. DANA 1/2022, 53 ff.).

Iran

Durchsetzung des Verhüllungszwangs mit automatischer Mustererkennung

Mit automatischer biometrischer Gesichtserkennung etwa in öffentlichen Verkehrsmitteln gehen Irans Machthaber gegen Frauen vor, die ihr Gesicht nicht „korrekt“ verhüllen. Kameras sollen gemäß einer Ankündigung der zuständigen Moralbehörde des Landes dazu genutzt werden Frauen und Mädchen auszuspähen, die ihren Hidschab nicht korrekt tragen. Finanziert werden soll das Projekt aus den eingenommenen Geldstrafen. Bei Verletzung der Verhüllungsvorschriften sind sogar Haftstrafen und der Entzug grundlegender Bürgerinnenrechte sowie des Internetzugangs vorgesehen. Nach der islamischen Revolution 1979 wurde der Hidschab-Zwang für alle Frauen und Mädchen, die älter als neun Jahre sind, eingeführt.

Biometrische Ausweise ermöglichen die Durchsetzung der Verhüllungsvorschriften mittels Gesichtserkennung. Für immer mehr Bedürfnisse ist der Einsatz biometrischer Ausweise verpflichtend. Damit verfügt die Regierung über eine Datenbank mit Irismustern, Gesichtern und Fingerabdrücken der meisten Einwohner Irans. Diese Datenbank wird nun zur schärferen Unterdrückung von Frauen und Mädchen genutzt.

Während sich das Land in einer schweren Wirtschaftskrise mit extremer Inflation befindet, verschärft die speziell zuständige Polizeibehörde ihr Vorgehen gegen vermeintlich unmoralisch gekleidete Frauen und Mädchen. Hierbei soll es auch schon zu Schusswaffengebrauch gekommen sein. Selbsternannte Moralapostel attackieren vermeintliche Übeltäterinnen in der Öffentlichkeit. Die öffentliche Hand gibt laut einem Bericht um die 200 Millionen Dollar jährlich für Hidschab-Propaganda aus.

Am 15.08.2022 hat Staatspräsident Ebrahim Raisolsadati die Vorschriften per Dekret weiter verschärft, offenbar mit der Zielsetzung das Geldstrafenaufkommen zu steigern, das ins Budget der Moralbehörde fließt. Neben den „Übeltäterinnen“ selbst sollen auch

Gebäudebesitzer bestraft werden, wenn ihre Gebäude von nicht ordnungsgemäß Verhüllten frequentiert werden. Ebenso werden Hausmeister bestraft, wenn die Mieterinnen in ihrem Wirkungsbereich die Verhüllungsvorschriften nicht einhalten. Gleiches gilt für Behördenmanager in Bezug auf deren Mitarbeiterinnen.

Immer häufiger wurde Frauen unter dem Vorwand unmoralischer Kleidung der Zutritt zu Banken, Ämtern und öffentlichen Verkehrsmitteln verwehrt. Die Moralbehörde beantragte eine neue Bestimmung im Computerstrafrecht: Wer Bilder oder andere Inhalte online stellt, die „öffentlicher Sittsamkeit entgegenstehen", oder wer sich im Netz einfach nur gegen den Hidschab-Zwang ausspricht, soll mit Geldstrafen sowie bis zu zwei Jahren Haft bestraft werden können. Für den Upload von Bildern iranischer Frauen ohne Hidschab ist der Entzug von Bürgerrechten vorgesehen, samt Verbot der Internetnutzung zwischen sechs Monaten und einem Jahr. Frauen im öffentlichen Dienst, deren „unislamische" Profilfotos im Netz aufgespürt werden, droht die Entlassung.

Kurz nach den Verschärfungen wurde bekannt, dass eine Frau, die von der Moralbehörde inhaftiert worden war, nachdem ihr unziemliches Tragen des Kopftuchs vorgeworfen wurde, tot war. Darauf entstanden die schwersten Proteste, die es im Iran seit Jahren gab, bei denen viele Frauen und junge Mädchen ihr Haar frei trugen und gegen den Kopftuchzwang z.B. durch Verbrennen der Tücher protestierten (Sokolov, Iran: Gesichtserkennung soll Frauen in Hidschab zwingen, www.heise.de 07.09.2022, Kurzlink: https://heise.de/-7255428).

Südkorea

Datenschutzstrafgelder gegen Google und Meta

Google und der Facebook-Mutterkonzern Meta sollen in Südkorea wegen Verstößen gegen das Datenschutzgesetz Strafen in zweistelliger Millionenhöhe zahlen. Die Kommission zum Schutz persönlicher Daten (PIPC) warf beiden Unternehmen am 14.09.2022 vor, sie hätten Kundendaten für personalisierte Online-Werbung genutzt ohne vorher deren Zustimmung eingeholt zu haben. Die Nutzenden seien nicht ausreichend informiert worden, dass ihre Daten dafür gebraucht würden. Google soll 69,2 Milliarden Won (49,7 Mio. Euro) und Meta 30,8 Milliarden Won (22,1 Mio. Euro) Strafe zahlen.

Die Beträge stellten die höchsten Geldstrafen dar, die wegen Datenschutzverstößen in Südkorea verhängt worden sind, hieß es in einer Mitteilung der unter der Aufsicht des südkoreanischen Präsidenten stehenden Kommission. PIPC wies die US-Konzerne an ihr Verhalten zu korrigieren. Beide Unternehmen müssten die Nutzenden klar informieren und deren Zustimmung erfragen, falls sie Daten über das Verhalten ihrer Kunden auf Websites oder in Anwendungen verfolgten und sammelten.

Ein Sprecher von Meta kritisierte die Entscheidung und deutete an nötigenfalls vor Gericht zu ziehen: „Wir respektieren die Entscheidung von PIPC, doch sind überzeugt, dass wir mit unseren Kunden in rechtskonformer Weise zusammenarbeiten." Alle Vorgaben würden erfüllt. Meta sei für alle Optionen einschließlich eines Gerichtsbeschlusses offen (Datenschutz: Südkorea belegt Google und Meta mit Millionen-Strafen, www.heise.de 14.09.2022, Kurzlink: https://heise.de/-7263773).

China

NSA wird der Netzwerkspionage beschuldigt

Mitarbeiter vom US-Geheimdienst NSA (National Security Agency) sollen sich gemäß der chinesischen, staatlich unterstützten Zeitung Global Times die Kontrolle über Teile des chinesischen Telekommunikationsnetzes verschafft haben. Die NSA habe sich über einen E-Mail-Phishing-Angriff auf eine staatlich mitfinanzierte Universität Zugriff verschafft. Peking sieht demgemäß die Abteilung für Cyber-Kriegsführung der USA, namentlich den US-Auslandsgeheimdienst NSA, als Angreifer. Bereits im Juni 2022 war ein Phishing-Angriff auf Angehörige der Northwestern Polytechnical University bekannt geworden. Lehrkräfte und Studenten sollen damals E-Mails mit Trojanern erhalten haben, über die an persönliche Daten gelangt werden sollte.

Der NSA soll es nach Angaben der Global Times darüber gelungen sein Fernzugriff auf die Kernnetzwerke der Universität und einen Zugang zu den Telekommunikationsbetreibern erlangt zu haben. Dabei seien sensible Daten, unter anderem Netzwerkkonfigurationen, Netzwerkverwaltungsdaten und Betriebsdaten erbeutet worden. Wie die Angreifer im Detail vorgegangen sind und von dem Netz der Universität den Zugriff auf Teile des chinesischen Telekommunikationsnetzes erlangen konnten, verrät die Global Times nicht. Eine Analyse der Malware hätte aber ergeben, dass der Angriff auf das Data Reconnaissance Bureau der Informationsabteilung der US-amerikanischen NSA zurückgehe. Unklar blieb, welche Telekommunikationsbetreiber konkret betroffen waren.

Das chinesische Telekommunikationsnetz befindet sich weitgehend in den Händen von den drei großen Betreibern China Mobile, China Unicom und China Telecom, sodass mutmaßlich einer oder mehrere dieser Betreiber betroffen sein könnten. Die USA und China werfen sich in den letzten Jahren immer wieder gegenseitig Wirtschaftsspionage und allgemein das Eindringen in Netze und Ausspähen von Daten vor. China beschuldigt dabei zunehmend staatliche Stellen der USA als Angreifer (Bünte, US-Geheimdienst soll ins chinesische Telekommunikationsnetz eingedrungen sein, www.heise.de 22.09.2022, Kurzlink: https://heise.de/-7272274)

Vietnam

Speicherpflicht von Internet-Nutzungsdaten

Vietnams Regierung hat Telemedien- und Telekommunikationsfirmen verpflichtet ab dem 01.10.2022 Daten ihrer Nutzenden zu speichern. Die per Erlass am 17.08.2022 veröffentlichten Regeln sollen für soziale Netzwerke wie Facebook, Internetkonzerne wie Google sowie Telekommunikationsanbieter gelten. Es gehe um die Daten aller Internetnutzer, „von Finanz-, über biometrische Daten hin zu Informationen über die

ethnische Zugehörigkeit und die politischen Ansichten". Auch alle Daten, die beim Surfen im Internet anfallen, sollen vor Ort vorgehalten werden. Ausländischen Firmen bleiben gemäß Presseberichten 12 Monate, um nach Inkrafttreten der Regeln die lokale Datenspeicherung umzusetzen und dafür verantwortliche Büros einzurichten. Die Daten müssen mindestens 24 Monate gespeichert werden. Vietnamesischen Behörden wird derweil erlaubt „Daten für Ermittlungszwecke anzufordern" und die Entfernung von Inhalten zu verlangen, sollten diese gegen die Richtlinien der Regierung verstoßen. Die in Vietnam vertretene Facebook-Mutter Meta und Google äußerten sich zunächst nicht zu den neuen Regularien.

Vietnam wird seit Jahrzehnten von der Kommunistischen Partei (KPV) dominiert, der einzigen legalen Partei im Land. Diese sorgt für strikte Internetkontrolle; immer wieder gibt es drakonische Strafen für online getätigte Meinungsäußerungen. 2020 hatten Provider in dem Land Facebook so lange abgeklemmt und das Portal unbenutzbar gemacht, bis sich der US-Dienst bereit erklärte „staatsfeindliche" Inhalte deutlich schärfer zu zensieren. In Bezug auf die Pressefreiheit listete Reporter ohne Grenzen das Land zuletzt auf Platz 174 von 180. Vor Vietnam hat beispielsweise Russland ausländische IT-Konzerne dazu verpflichtet Nutzungsdaten im Land zu speichern (Mai, Hanoi greift nach den Nutzerdaten, taz 22.08.2022; Holland, Vietnam: IT-Konzerne müssen alle Daten über ihre Nutzer im Land speichern, www.heise.de 18.08.2022; Kurzlink: https://heise.de/-7235468).

Technik-Nachrichten

Abmahnungen wegen Einbindung von Online-Google-Fonts

Tausende Empfänger erhielten Forderungsschreiben in ihrem E-Mail-Postfach oder im Briefkasten, weil sie Googles kostenlose Fonts in ihre Websites eingebettet haben und deshalb 100 € bis knapp 500 € bezahlen sollen. Die Abmahnungen werfen ihnen einen „unzulässigen Eingriff in das allgemeine Persönlichkeitsrecht" und einen Verstoß gegen die Datenschutz-Grundverordnung (DSGVO) vor. Bei Google-Fonts handelt es sich um ein Verzeichnis von mehreren Hundert frei verwendbarer Schriftarten. Website-Betreiber können die Schriftarten herunterladen und lokal auf dem eigenen Webserver bereitstellen. Alternativ dazu können sie die Schriften auch online einbinden. Dies führt dann dazu, dass der Browser des Besuchers sie beim Aufruf einer Seite von den Servern des US-Konzerns lädt, was rechtlich problematisch ist.

• Rechtlicher Hintergrund

Das Landgericht (LG) München I hatte im 20.01.2022 die Online-Nutzung von Google Fonts mit der Begründung verboten, dass dabei unerlaubt personenbezogene Daten an Google in die USA weitergegeben werden (Az. 3 O 17493/20). Diese Entscheidung bildet die Grundlage für die versandten Abmahnungen und Forderungsschreiben. Es handelt sich bei den übermittelten dynamischen IP-Adressen um Informationen, die in den Schutzbereich des Datenschutzes fallen. Der Seitenbetreiber habe das Recht des Klägers auf informationelle Selbstbestimmung verletzt, indem er die dynamische IP-Adresse des Besuchers beim Aufruf der Seite an Google weiterleitete. Hierfür habe es keine Rechtsgrundlage in Form einer Einwilligung oder eines berechtigten Interesses gegeben. Dem Kläger stehe somit ein Unterlassungsanspruch zu.

Zudem hatte das LG München I dem Besucher der Website noch einen Schadensersatzanspruch in Höhe von 100 € zugebilligt. Ein solcher Anspruch kann sich aus Artikel 82 der DSGVO ergeben und steht jeder Person zu, „der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist". Die Frage, welche Intensität ein solcher Eingriff haben muss, um ein Schmerzensgeld auszulösen, ist sehr umstritten. In der juristischen Diskussion wird die Entscheidung aus München überwiegend als überzogen kritisiert. Die Richter sahen im vorliegenden Fall bereits durch die Übermittlung an Google einen „Kontrollverlust" des Betroffenen und ein „individuelles Unwohlsein". Denn Google sei bekannt dafür Daten über seine Nutzer zu sammeln. Zudem sei es unstreitig, dass die IP-Adresse an einen Server in den USA übermittelt werde, wo kein angemessenes Datenschutzniveau gewährleistet sei.

Diese Argumentation machen sich jetzt die Absender der Abmahnungen zu eigen. Man habe die Website des Empfängers besucht, dieser verwende die Online-Version der Google Fonts und solle daher wegen des dadurch verursachten individuellen Unwohlseins schnellstens 100 € an den Versender überweisen. Kommt das Schreiben von einem Anwalt, so fordert dieses, dass die Empfänger den Schaden ihrer Mandanten begleichen, eine Unterlassungserklärung für die Nutzung der Google-Fonts abgeben und die Anwaltsgebühren, meist in Höhe von ca. 370 €, zahlen sollen.

Gegen die anwaltlichen Abmahnungen gibt es eine ganze Reihe von potenziellen Einwendungen, sodass es sich dabei keinesfalls um „sichere Fälle" für die Abmahner handelt. Es spricht einiges dafür, dass die Anwaltsschreiben rechtsmissbräuchlich sind, da die angeblichen Betroffenen die Websites vorsätzlich angesteuert haben dürften. Trotzdem sollten zumindest juristische Laien in diesen Fällen vorsichtshalber

einen IT-Anwalt ins Boot holen. Kommen die Aufforderungsschreiben nicht von einem Anwalt, dann ist es eher unwahrscheinlich, dass die Mehrheit der Gerichte den Ansichten des LG München hinsichtlich der Zahlung einer Geldentschädigung folgen. Es spricht einiges dafür, dass man derartige Schreiben ignorieren kann. Allerdings sollte jeder Website-Betreiber auf die lokal gehostete Version von Google Fonts umsteigen.

• Anrüchige Spendenaktion

Bei einer der Abmahnenden handelt es sich um eine „Interessengemeinschaft Datenschutz" (IG Datenschutz), hinter der ein Martin Ismail aus Hannover und dessen Anwalt Kilian Lenard aus Berlin stecken. Lenard bezeichnet sich auf seiner eigenen Website als kompetenter Ansprechpartner für Datenschutz und IT-Recht. Ausweislich seiner Website ist Kilian Lenard seit über 20 Jahren auf dem Gebiet des Internetrechts tätig und begleitet seine Mandanten seit 1997 erfolgreich, wobei der besondere Fokus seiner Beratung auf Startups und Technologiefirmen liege. Über Martin Ismail ist nicht viel bekannt. Er wird auf der Website der IG Datenschutz als Verantwortlicher genannt. Angeblich tritt die IG Datenschutz für den Datenschutz und die Privatsphäre im Internet ein. Man beobachte, dass zwar verschiedene Maßnahmen getätigt wurden, es aber leider noch viele Bereiche gäbe, bei denen die DSGVO nicht umgesetzt werde.

Vom 29.09.2022 warb die IG Datenschutz für sich auf ihrer Webseite damit, dass sie gemeinnützige Organisationen mit Spenden in Höhe von jeweils 3.060 € unterstütze – und zwar die Deutsche Vereinigung für Datenschutz e.V. (DVD) und den Deutschen Kinderverein e.V. Als der DVD-Vorstand feststellte, dass mit dem Namen der Bürgerrechtsvereinigung Werbung für die IG gemacht wurde, wandte sich die DVD mit folgendem Schreiben an die IG Datenschutz:

Sehr geehrte Herren Ismail und Lennard,

mit großer Verärgerung mussten wir feststellen, dass Ihre „großzügige" Spende für die DVD in Höhe von 3.060 € auf eine rechtsmissbräuchliche Abmahnung von oft gutgläubigen und unbedarften Webseitenbetreibern zurückgeht. Der DVD-Vorstand hat beschlossen das Geld nicht anzunehmen und fordert Sie auf umgehend Ihre Behauptung auf der Webseite https://igdatenschutz.de/spenden zu unterlassen, die angeblich bedachte DVD verfolge „ein sehr ähnliches Ziel wie die IG Datenschutz, weswegen wir mit Spenden ihr Arbeit unterstützen möchten". Ihr unseres Erachtens unzulässiges Vorgehen schadet der DVD als Verein und dem Anliegen des Datenschutzes generell. Die DVD wird sich mit den ihr zur Verfügung stehenden Mitteln dagegen zur Wehr setzen mit Ihrer Abmahnaktion in Verbindung gebracht zu werden. Teilen Sie uns eine Kontoverbindung für die Rücküberweisung mit.

Außerdem fordern wir Sie auf, umgehend Ihre Abmahnaktivitäten zu beenden. Teilen Sie uns mit, wieviele Webseitenbetreiber Ihrer Zahlungsaufforderung bisher nachgekommen sind.

Gruß, Frank Spaeing, Heinz Alenfelder, Thilo Weichert

Der überwiesene Betrag wurde von der DVD umgehend zurücküberwiesen. Tatsächlich taucht die DVD auf der Webseite der IG-Datenschutz seit dem 04.10. 2022 nicht mehr auf. Eine Antwort auf ihre Fragen erhielt die DVD aber nicht. Der Deutsche Kinderverein e.V. folgte dem Beispiel der DVD. Als neuer Spendenempfänger wurde seit dem 30.09.2022 der Cybermobbing-Hilfe e.V. aufgeführt. Die Cybermobbing-Hilfe folgte dem Vorgehen der DVD und des Kindervereins. Der Vorsitzende des Vereins, Lukas Pohland, erklärt die Entscheidung des Vereins: „Bei Förderungen ist es uns wichtig, dass diese konzeptionell zu unserer Philosophie passen. Das sehen wir hier nicht".

• Trittbrettfahrer und Widerstand

Die „Interessengemeinschaft Datenschutz" ist nicht die einzige Pseudo-Datenschutzorganisation, die sich mit dieser anrüchigen Methode eine goldene Nase besorgt. Unter dem Namen VIVA Datenschutz mahnt z.B. die RAAG Kanzlei des Dikigoros Kairis für einen Herrn und eine Frau Wang Yu Online-Google-Fonts ab. Gefordert wurde hier eine Zahlung eines Schmerzensgeldes in Höhe von 140 €, „entstandene Anwaltskosten" in Höhe von 50 € zuzüglich Umsatzsteuer, womit sämtliche Ansprüche per Vergleich geklärt sein sollen. Verwiesen wird darin auf angeblich erstellte Trackingprotokolle, welche in einem Anhang ersichtlich sein sollen, der aber den Schreiben nicht beigefügt war. Weitere Abmahnaktionen gegen Webseiten mit Online-Google-Fonts folgten.

Dass die rechtliche Abwehr der Abmahnversuche erfolgreich sein kann, zeigt eine einstweilige Verfügung des Landgerichts Baden-Baden, das mit Beschluss vom 11.10.2022 auf Antrag eines Abmahnopfers unter Androhung eines Ordnungsgeldes von 5 Euro bis zu 250.000 Euro und unter Festsetzung eines Streitwertes von 30.000 Euro Ismail untersagt „einen Partnerbetrieb des Franchise-Systems der Antragstellerin mit Forderungen im Zusammenhang mit der Einbindung von ‚Google Font' zu kontaktieren" (Az. 3 O 277/22) (Heidrich, Angeblicher DSGVO-Verstoß: Abmahnwelle wegen Google Fonts, www.heise.de 09.08.2022, Kurzlink: https://heise.de/-7206364; www.abofalle-anwalt.de, 29.09.2022, Abmahnung Kilian Lenard für Martin Ismail wegen Google Fonts; Mühlenmeier, Datenschutzvereine sehen sich instrumentalisiert, www.golem.de 05.10.2022; Loschelder, Abmahnung Wang Yu und Schadensersatz, VIVA Datenschutz – eine Interessengemeinschaft Datenschutz? www.anwalt.de 10.10.2022; Recker, Update: Abmahnung der RAAG Kanzlei wegen Google Fonts, www.anwalt.de 11.10.2022; Weiß, Neue Abmahnwelle: Wieder gehen Schreiben wegen Google Fonts und DSGVO raus, www.heise.de 27.10.2022, Kurzlink: https://heise.de/-7322064; siehe hierzu auch die DVD-Presseerklärung in diesem Heft, S. 249).

CCC knackt Video-Ident-Verfahren

Der Chaos Computer Club (CCC), dessen Mitgliedern sich zur Aufgabe gemacht haben Sicherheitslücken aufzudecken, hat eine solche beim sogenannten Video-Ident-Verfahren nachgewiesen. Wer heute online zum Beispiel eine Versicherung abschließt oder ein Konto bei einer Bank eröffnen will, kann sich

bei vielen Anbietern per Video-Ident anmelden: Den Ausweis in die Computer- oder Handykamera halten, das geht schnell und erspart den Gang etwa in eine Post-Filiale.

• Die Methode des CCC

Der CCC belegt, dass es möglich ist eine falsche Identität vorzutäuschen. Damit würde man Konten eröffnen können oder auch Zugang erhalten zur elektronischen Gesundheitsakte. Mit etwas Farbe und einer Open-Source-Software konnten die Verfahren von sechs nationalen und internationalen Anbietern überlistet werden. Wer sie sind, wurde vom CCC nicht genannt. Stattdessen fordert der CCC in einer Pressemitteilung die Verfahren generell „nicht mehr dort einzusetzen, wo ein hohes Schadenspotential besteht".

Um für eine Identifizierung per Video die falsche Identität vorzutäuschen, filmt der Täuscher einen Ausweis aus mehreren Richtungen. Die Plastikkarte liegt dafür auf einer speziellen Platte mit Markierungen. Damit sein Bild und der gewünschte Name auf dem Ausweis erscheint, schneidet er diese am Computer aus einem zweiten abgefilmten Ausweis mit spezieller Software aus. Während er den ersten Ausweis in die Kamera hält, sieht der Mitarbeiter, der die Identität prüfen soll, auf seinem Bildschirm ein ganz anderes Bild. Denn das Bild des echten Ausweises wird per Software überlagert von den Fälschungen, die auf einem handelsüblichen Fernseher angezeigt und von dort ein zweites Mal abgefilmt werden. Und dieses Bild kommt bei dem Identifizierer an. Die vom CCC genutzten Ausweispapiere wurden von Testpersonen zur Verfügung gestellt, deren Identität nicht preisgegeben wurde.

Der CCC forderte: „Es wird Zeit für ein Ende der Beweislastumkehr: Nicht die Betroffenen sollten Schwächen der Systeme nachweisen müssen, die Verfahrensbetreiber sollten vielmehr verpflichtet werden deren Sicherheit nach anerkannten Regeln zu belegen. Die Erfüllung bestehender und neuer Anforderungen sollte künftig durch unabhängige Tests unter realen Angriffsbedingungen regelmäßig nachgewiesen werden. Insbesondere bedarf jede Aussage zur Wirksamkeit von Gegenmaßnahmen gesicherter Evidenz. Die bloße Behauptung, man habe etwas KI drübergesprenkelt, darf nicht mehr ausreichen."

• Offizielle Reaktionen

Die Gematik, zuständig für die Digitalisierung des Gesundheitswesens, hat das Video-Ident-Verfahren für die elektronische Patientenakte nach dem Bekanntwerden des Versuchs des CCC gestoppt. Das Bundesgesundheitsministerium begrüßte das am 09.08.2022 durch die Gematik ausgesprochene, vorläufige Verbot der Video-Identifikation: Gerade Patienten- und Behandlungsdaten seien hochsensible Daten, deswegen sei das BMG um hohe Sicherheitsstandards bemüht.

Auch das Bundesinnenministerium zeigte sich kritisch: „Das Video- und Autoidentifizierungsverfahren ist grundsätzlich eine Brückentechnologie, die aufgrund ihrer Marktdurchdringung und Verfügbarkeit derzeit zur Fernidentifizierung genutzt wird." Man nehme die vom CCC dokumentierten Angriffsvektoren sehr ernst und wolle sorgfältig prüfen – und danach auch die Zukunft von Videoident insgesamt beurteilen. Das dem Bundesinnenministerium nachgeordnete Bundesamt für Sicherheit in der Informationstechnik (BSI) bekräftigte kritisch: „Bei videobasierten Fernidentifikationslösungen ist grundsätzlich eine Manipulation des Videostreams möglich, sodass videobasierte Lösungen nicht dasselbe Sicherheitsniveau erreichen können wie beispielsweise die Online-Ausweisfunktion des Personalausweises. Die Entscheidung, inwiefern das Video-Ident-Verfahren in anderen Anwendungsgebieten unter den gegebenen Umständen weiterbetrieben werden kann, liegt in der Zuständigkeit der jeweiligen Aufsichtsbehörden."

• Kritik aus der Finanz- und Digitalwirtschaft

Das Video-Ident-Verfahren gibt es schon seit Jahren. Gerade Jüngere nutzen das Verfahren bei Online-Banken wie N26, aber auch Großbanken oder Sparkassen machen mit. Ein Banker eines großen deutschen Instituts sagte: „Video-Ident stirbt gerade." Offiziell dagegen beschwichtigen die Banken und weisen auf die Sicherheit des Verfahrens hin, das schließlich schon seit Jahren eingesetzt werde. Gemäß einer journalistischen Umfrage plante zunächst keine namhafte Bank in Deutschland das Video-Ident-Verfahren zu stoppen. Die Deutsche Kreditwirtschaft, Deutschlands wichtigster Interessenverband für Finanzinstitute, ließ wissen, das Verfahren werde „beanstandungsfrei genutzt" und sei zuletzt 2022 von der Bafin überprüft und für gut befunden worden. Gemäß dem Bankenverband bestehen weitere Maßnahmen unter anderem darin, dass Neukunden über sechs bis zwölf Monate einem strengen Transaktionsmonitoring unterliegen würden, so eine Sprecherin, „Die Entscheidung der Krankenkassen das Verfahren nicht zu nutzen, muss nicht automatisch Rückschlüsse auf Anwendungen in anderen Sektoren haben."

Eine Sprecherin der Bafin erklärte: „Hinweise auf Sicherheitsprobleme oder Schwachstellen in Bezug auf das Identifizierungsverfahren nehmen wir sehr ernst." Allerdings sei eine abschließende Bewertung der Angriffsszenarien kurzfristig nicht möglich, da „maßgebliche" Einzelheiten noch nicht bekannt seien. Sollte es zu einer Einschränkung kommen, wird das insbesondere die Banken hart treffen, die keine oder nur wenige Filialen haben.

Auch in der Versicherungswirtschaft herrscht Aufregung; ein einheitliches Vorgehen zeichnete sich nicht ab. Während der Gesamtverband GDV auf die Bafin verwies, bietet der genossenschaftliche Versicherer R+V Video-Ident zunächst nicht mehr an, steht aber im Kontakt mit seinem Video-Ident-Anbieter, um auszuloten, „mit welchen weiteren Maßnahmen die Sicherheit noch weiter verbessert werden kann".

Für die Branche der Video-Ident-Anbieter kam der Vorstoß des Chaos Computer Clubs überraschend. Sie hätten sich gewünscht, so Vertreter der Branche, vorab über die Lücke informiert zu werden. Das sieht der für den Hack verantwortliche CCC-Sicherheitsforscher Martin Tschirsich anders. Dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sei diese Angriffsmöglichkeit schon lange bekannt, daher habe man die Behörde am 08.08.2022

nur darüber informiert, dass man in Kürze die Meldung über den erfolgreichen Hack veröffentlichen werde. Gemäß Tschirsich wurde die Aktion schon „seit Längerem" vorbereitet. Ziel sei es gewesen zu zeigen, dass die theoretisch bekannte Lücke tatsächlich in der Praxis ausgenutzt werden kann und dass dies den Anbietern auch im Nachhinein nicht auffalle. Alle eröffneten Konten oder Zugänge hätten bei der Bekanntgabe noch funktioniert. Den Aufwand, der für die Überwindung der Sicherheitsmechanismen getrieben werden muss, hält Tschirsich für lediglich „moderat".

Sehr kritisch reagierte der Digital-Verband Bitkom auf die Entscheidung der Gematik Video-Ident sofort zu stoppen: „Wegen einzelner Sicherheitsvorfälle, die sich in der digitalen Welt ebenso wenig ausschließen lassen wie in der analogen Welt, darf man (...) nicht wie mit einem Bulldozer das Video-Ident-Verfahren als solches plattmachen." Anderswo sei man bereits weiter, so der Verband: „Länder wie Dänemark machen uns vor, wie sich Bürgerinnen und Bürger einfach, sicher und vertrauensvoll digital identifizieren können" (Borchers, Chaos Computer Club hackt Videoident-Verfahren, www.heise.de 10.08.2022, Kurzlink: https://heise.de/-7216044; Steiner, Nach Videoident-Hack: Alle prüfen, Banken vertrauen vorerst weiterhin, www.heise.de 11.08.2022, Adchayan/Martin-Jung/Wischmann, Ich bin's. Oder doch nicht? SZ 15.08.2022, 15).

Boarding-Pass eröffnet Zugang zu sensiblen Daten

Über den QR-Code auf einem Fluglinien-Boardingpass können Fremde Zugang auf Daten des Passagiers erlangen, darunter seine E-Mail-Adresse und seine Handynummer.

Weil sie sensible Daten enthält, so der Ratschlag der Lufthansa, solle man seine Bordkarte „wie Bargeld" behandeln. Carsten Spohr, Chef der Fluglinie, hat sich offenbar nicht daran gehalten und wurde deshalb zum Opfer eines Datendiebstahls.

Boarding-Pässe ermöglichen den Zugang zu Informationen, die über einen konkreten Flug hinausgehen, auch sensible Daten, etwa die Servicekartennummern von Vielfliegern. Gemeinsam mit dem Nachnamen des jeweiligen Kunden lassen sich darüber auf der Lufthansa-Website die jeweils anstehende Buchung auslesen, Bordkarten drucken oder Versandarten für die Einsteigedokumente verändern. Eine zusätzliche PIN wird lediglich für das Einloggen ins Nutzerprofil des Kunden benötigt.

Gemäß einem Lufthansa-Sprecher ist dem Unternehmen bewusst, dass sich über die im Boarding-Pass enthaltenen Informationen Daten über eine aktuelle Buchung und etwaige Handynummern oder E-Mail-Adressen auslesen lassen, sofern diese hinterlegt sind. Ein Sicherheitsrisiko liege zwar „nicht vor", jedoch arbeite das Unternehmen über eine Geschäftseinheit namens „Digitaler Hangar" an neuen Standards für die Industrie. Der Schutz der Daten liege in den Händen der Kundschaft: „Wir empfehlen unseren Fluggästen, grundsätzlich sehr sorgsam mit den Flugdokumenten umzugehen. Sie sind wie Bargeld zu behandeln." An diesen Ratschlag hatte sich Spohr offenbar nicht gehalten, so dass Unbekannte seine Daten abfragten (Fremde hatten Zugriff auf Daten von Lufthansa-Chefs, www.spiegel-online.de 23.09.2022 = Lufthansa-Boss wird Opfer von IT-Lücke, Der Spiegel Nr. 39, 24.09.2022, 63).

KI soll Ertrinkende in Schwimmbad detektieren

Bäderbetriebe in München und Wiesbaden erproben ein israelisches Überwachungssystem mit Kameras und Bewegungserkennung, das in Not geratene Badende vor dem Ertrinken retten können soll. Bei verdächtigen Situationen schlägt die integrierte, laut Herstellerangaben auf Maschinenlernen basierende Technik Alarm bei der Badeaufsicht über eine Smartwatch. So sollen Rettungsschwimmer schneller zielgerichtet Hilfe leisten können.

Die Stadtwerke München (SWM) haben Ende Juli 2022 im Südbad das Pilotprojekt „Smartes Schwimmbad" gestartet. Im Zuge der üblichen Instandhaltungs- und Reparaturmaßnahmen wurde „eine neue Technik für alle Becken eingebaut", so das kommunale Versorgungs- und Dienstleistungsunternehmen: „Künstliche Intelligenz soll dabei unterstützen Bewegungsmuster im Wasser auch datengesteuert zu erkennen." Nach einer mehrwöchigen Testphase wurden die Kameras scharf gestellt. In einem rund zweijährigen Pilotprojekt wollen die SWM so Erkenntnisse gewinnen, ob die Technik für alle von ihnen betriebenen Bäder „nutzbringend" ist. SWM-Mitarbeiter Max Fuchs meint: „Die digitale Hilfe gibt den Kollegen am Becken mehr Sicherheit." An der Konzentration der Badeaufsicht ändere sich durch die Unterstützung nichts, die künstliche Intelligenz (KI) könne Rettungsschwimmer nicht ersetzen: „Im schlimmsten Fall müssen wir die Schwimmer ja aus dem Wasser retten. Das kann die Technik nicht."

Das eingesetzte System stammt von der Firma Lynxight aus Tel Aviv. Es besteht aus zwei Komponenten: Die eingesetzten Kameras sollen im ersten Schritt die Bewegungen im Wasser aufzeichnen, so die SWM: „Sie erfassen keine Echtbilder einzelner Personen – also auch keine Gesichter." Details der Aufnahmen rechne die Lösung in Vektordaten um und leite daraus Bewegungsmuster ab. Anschließend würden die Bilder sofort gelöscht. Die Kamerawinkel reichten über die gesamte Wasserfläche. Gekoppelt sind die elektronischen Augen mit Smartwatches für das Aufsichtspersonal vor Ort. Diese sollen in Echtzeit und mit genauer Positionsangabe warnen können, falls die Bewegung im Wasser nach rund 20 Sekunden auf eine ungewöhnliche Lage und mögliche Gefahr hindeutet. Schwimmer können zudem gemäß der SWM gezählt werden: „Darüber hinaus ist es möglich anhand der über längere Zeiträume gewonnenen Vektordaten zu analysieren, wie sich die Auslastung in den Becken darstellt."

Laut dem Münchner Versorgungsbetrieb ist das System mit der Datenschutz-Grundverordnung (DSGVO) vereinbar. Die Besucher des Hallenbads in Sendling, bei dem bei schönem Wetter die Tore der Fassade versenkt werden, würden im Eingangsbereich sowie beim Betreten der Schwimmhalle schriftlich über die KI-Kontrolle informiert. Das System arbeitet noch nicht fehlerfrei und absolvierte zunächst eine 60 Tage dauernde Lernphase. So kann das

System nicht zwischen Personen unterscheiden, die sich im Wasser bewegungslos sonnen, oder Schwimmern, die Hilfe benötigen. Falsche Warnungen seien die Folge. In solchen Fällen könnten die Bademeister über ihre Uhren ein Feedback geben und die KI so trainieren: „Das System lernt mit jeder Aktion dazu und soll dadurch im Verlauf des Projekts immer konkretere Vorhersagen und Klassifikationen treffen." So solle die künstliche Intelligenz die Rettungsschwimmer bald auch in Situationen unterstützen können, „in denen Spiegelungen, Blasen oder Schatten im Wasser oder auch die Menge an Personen die Lage unübersichtlich machen". Trotz der Anfangsschwächen zeigt sich die Aufsicht im Südbad begeistert. Besonders an vollen Tagen helfe das System schon jetzt sehr, auch wenn es noch keinen richtigen Notfall gegeben habe. Die Besucher hätten es bisher kaum bemerkt. Die von anderer Seite bereits erhobenen Datenschutzbedenken habe noch keiner geäußert.

Das Wiesbadener Frei- und Hallenbad Kleinfeldchen fühlt dem per WLAN vernetzten System schon seit einigen Monaten auf den Zahn. Der dortige Betriebsleiter Thomas Baum lobt es als „drittes Auge", das alle Ecken immer im Blick habe und wertvolle Unterstützung am Beckenrand liefere. Lynxight rechnet vor: „Die typischen medizinischen Kosten für ein Opfer eines Beinahe-Ertrinkens reichen von 75.000 US-Dollar für die Erstbehandlung bis zu 180.000 US-Dollar pro Jahr für die Langzeitpflege. Die Gesamtkosten bei einer Hirnverletzung in so einem Fall könnten mehr als 4,5 Millionen US-Dollar betragen." Die Überwachung eines Beckens mit der Lösung schlage im Monat dagegen nur mit 800 US-Dollar zu Buche. 85% der erfassten tödlichen Schwimmunfälle ereigneten sich laut der Deutschen Lebens-Rettungs-Gesellschaft (DLRG) 2021 aber nicht in öffentlichen Schwimmbädern, sondern in Binnengewässern wie Seen und Flüssen (Rek, Künstliche Intelligenz als Lebensretter, www.sueddeutsche.de 18.08.2022; Krempl, KI: Smarte Kameras sollen Menschen in Schwimmbädern vor dem Ertrinken retten, www.heise.de 20.08.2022, Kurzlink: https://heise.de/-7238396).

Kundendaten von Toyota waren 5 Jahre potenziell öffentlich abrufbar

E-Mail-Adressen und Kundenverwaltungsnummern von Nutzern von Toyotas T-Connect-Plattform waren fünf Jahre lang potenziell für jedermann abrufbar, weil ein Zugangsschlüssel beim Webdienst zur Softwareentwicklung GitHub öffentlich zugänglich war. Über die T-Connect-App können Autobesitzer ihre Smartphones mit dem Infotainmentsystem des Autoherstellers koppeln. Der Sourcecode der App findet sich auf GitHub und beinhaltete fünf Jahre lang einen Schlüssel, mit dem man auf Datenserver mit Kundeninformationen hätte zugreifen konnten. Gemäß Toyota waren davon 296.019 Nutzende betroffen. Bislang seien keine Fremdzugriffe dokumentiert, auszuschließen seien solche aber nicht vollständig. Namen, Kreditkartendaten und Telefonnummern sollen nicht unter den Informationen gewesen sein, da diese sich auf anderen Servern befinden. Verantwortlich für das Leck sei ein T-Connect-Subunternehmer, der den Quellcode irrtümlicherweise öffentlich verfügbar gemacht hatte. Toyota entschuldigte sich für den Vorfall; seit dem 17.09.2022 seien auf diesem Wege keine Zugriffe mehr möglich.

Um solchen Leaks vorzubeugen, bietet GitHub die Option von „verschlüsselten Geheimnissen". Damit können Entwickler sensible Informationen abgeschottet in Repositories ablegen und so vor unberechtigten Zugriffen schützen. Außerdem scannt GitHub Projekte auf Authentifizierungsschlüssel und blockiert derartigen Code. Kommen hier aber benutzerdefinierte Schlüssel zum Einsatz, kann diese Schutzmaßnahme ins Leere laufen (Schirmacher, Datenpanne bei Toyota: Schlüssel zu Kundendaten fünf Jahre öffentlich zugänglich, www.heise.de 11.10.2022. Kurzlink: https://heise.de/-7304741).

Rechtsprechung

EuGH

Deutsche TK-Vorratsdatenspeicherung verstößt gegen europäische Grundrechte

Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 21.09.2022 bestätigt, dass die deutsche Regelung für eine allgemeine und unterschiedslose Vorratsdatenspeicherung von Telekommunikations-(TK-)Metadaten dem Unionsrecht widerspricht (C-793/19 und C-794/19). Die bisherige deutsche Regelung wird wegen rechtlicher Unsicherheiten seit 2017 nach einer Entscheidung des Oberverwaltungsgerichts Nordrhein-Westfalen nicht mehr angewandt (DANA 3/2017, 177 f.).

Mit Urteil vom 02.03.2010 hatte das Bundesverfassungsgericht schon früh eine deutsche Regelung zur TK-Vorratsdatenspeicherung aufgehoben (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08). Am 08.04.2014 kippte der EuGH die damals geltende europäische Regelung hierzu (C-293/12 und C-594/12). Am 05.04.2022 kassierte der EuGH eine entsprechende irische Regelung (DANA 2/2022, 125 f.), im Jahr 2020 die Gesetze von Großbritannien, Belgien und Frankreich (DANA 4/2020, 263 ff.).

• Das Urteil

Ausnahmsweise dürfen nach dem aktuellen Urteil Verkehrs- und Standortdaten sowie IP-Adressen gespeichert werden, wenn „eine ernste Bedrohung für die nationale Sicherheit" vorliegt: „Zur Bekämpfung schwerer Kriminalität können

die Mitgliedstaaten jedoch unter strikter Beachtung des Grundsatzes der Verhältnismäßigkeit insbesondere eine gezielte Vorratsdatenspeicherung und/oder umgehende Sicherung solcher Daten sowie eine allgemeine und unterschiedslose Speicherung von IP-Adressen vorsehen." In solchen Fällen kann das Telekommunikationsgesetz (TKG) die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste zu einer „allgemeinen und unterschiedslosen Vorratsdatenspeicherung eines Großteils der Verkehrs- und Standortdaten der Endnutzer dieser Dienste für eine Dauer von mehreren Wochen" verpflichten.

Das Bundesverwaltungsgericht hatte sich an den EuGH mit der Frage gewandt, ob das Unionsrecht den nationalen Rechtsvorschriften entgegensteht (DANA 4/2020, 237 f.), was das Gericht nun bestätigt: Es wird erlaubt Verkehrs- und Standortdaten auf Vorrat nur zu speichern, „wenn sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht". Ein Gericht oder eine unabhängige Verwaltungsstelle muss diese Anordnung kontrollieren, der Zeitraum ist begrenzt. Entsprechendes gilt, auch bei zeitlicher Begrenzung und Nachweis der Notwendigkeit, für die Bekämpfung schwerer Kriminalität und die Verhütung schwerer Bedrohungen der öffentlichen Sicherheit.

Ein besonderes Augenmerk legte der EuGH auf die Bekämpfung der Kinderpornografie. Weil „die IP-Adresse der einzige Anhaltspunkt sein kann, der es ermöglicht die Identität der Person zu ermitteln, der diese Adresse zugewiesen wurde", lässt das Gericht hier mehr Raum für eine Vorratsdatenspeicherung. Unter Beschränkung auf das „absolut Notwendige" und unter Einrichtung verfahrensmäßiger Sicherungen soll hier eine abgespeckte Version der Speicherung möglich sein.

Der mit dieser anlassbezogenen Vorratsdatenspeicherung verbundene Eingriff in die Grundrechte bedarf einer gesonderten Rechtfertigung. „Daraus folgt, dass nationale Rechtsvorschriften, die die vollständige Einhaltung der Voraussetzungen gewährleisten, die sich im Bereich des Zugangs zu auf Vorrat gespeicherten Daten aus der Rechtsprechung ergeben, naturgemäß den schwerwiegenden Eingriff in die Rechte der Betroffenen, der sich aus der allgemeinen Vorratsspeicherung dieser Daten ergeben würde, weder beschränken noch beseitigen können." Der EuGH bestätigt das zentrale Argument der Kritiker der Vorratsdatenspeicherung, dass nämlich genaue Schlüsse auf das Privatleben der Personen ermöglicht und Profile erstellt werden können. Dies könne auch unter den engen Voraussetzungen nicht vollständig verhindert werden.

Hintergrund des Urteils ist der Rechtsstreit zwischen der Bundesnetzagentur und dem Internetprovider Spacenet sowie der Telekom. Beide Unternehmen wehrten sich gegen die Vorschrift, bestimmte Daten speichern und diese Daten den Behörden zur Verfügung stellen zu müssen. Das zuvor erstellte Gutachten des EuGH-Generalanwalts hatte die nun erfolgte Entscheidung bereits inhaltlich vorskizziert. Der Fall geht nun zurück an das Bundesverwaltungsgericht, das einen EU-Rechtsverstoß der deutschen Regelung festzustellen hat. Die Bundesregierung muss letztlich ein neues Gesetz erarbeiten, worüber sich die Koalition bisher nicht einigen konnte.

• Reaktionen der Politik

Die stellvertretende Vorsitzende der Unionsfraktion, Andrea Lindholz (CSU), sagte: „Gut, dass nun endlich Klarheit herrscht." Sie forderte die Bundesregierung auf zügig einen Gesetzentwurf vorzulegen. Der bayerische Justizminister Georg Eisenreich (CSU) betonte die Erforderlichkeit von Daten im „Kampf gegen Kinderpornografie und sexuellen Kindesmissbrauch": „Die vom EuGH eingeräumten Spielräume für die Verkehrsdatenspeicherung insbesondere von IP-Adressen müssen vor allem zum Schutz der Kinder vor schweren Verbrechen genutzt werden. Jeder Fall, der nicht aufgeklärt und gestoppt werden kann, ist einer zu viel." Auch bei der Verfolgung von Terroristen, Waffenschiebern und Drogenhändlern seien IP-Adressen oft die wichtigste oder sogar die einzige Spur. Bayerns Innenminister Joachim Herrmann (CSU) ergänzte: „Ideologisch übertriebener Datenschutz wäre falsch verstandener Täterschutz. Das darf sich ein Rechtsstaat nicht leisten. Unsere Ermittler von Polizei und Justiz brauchen zur Bekämpfung bestimmter schwerer Straftaten unbedingt Verkehrsdaten wie IP-Adressen." Er werde die Auswirkungen des Urteils zu einem Schwerpunkt der gemeinsamen Sitzung der deutschen Innenminister und Justizminister am 27.09.2022 in München machen. Zuvor hatte sich Bundesinnenministerin Nancy Faeser (SPD) vor allem mit Blick auf den Kampf gegen sexuellen Kindesmissbrauch für eine auf IP-Adressen beschränkte Vorratsdatenspeicherung starkgemacht.

Bundesjustizminister Marco Buschmann (FDP) sprach angesichts des Urteils von einem „guten Tag für die Bürgerrechte". Der EuGH habe in einem historischen Urteil bestätigt: „Die anlasslose Vorratsdatenspeicherung in Deutschland ist rechtswidrig." Die Bundesregierung werde dieses Instrument daher „nun zügig und endgültig aus dem Gesetz streichen". Der parlamentarische Justizstaatssekretär Benjamin Strasser (FDP) meinte, mit „Quick Freeze" liege ein rechtssicheres Instrument auf dem Tisch. Bei diesem Verfahren sollen Telekommunikationsanbieter Verkehrsdaten bei einem konkreten Tatverdacht schnellstmöglich „einfrieren", um dann Täter identifizieren und sie der Strafverfolgung zuführen zu können. Sinnlose Debatten über eine „umetikettierte anlasslose Datenspeicherung sollten wir uns aufgrund des Koalitionsvertrages sparen".

Grünen-Fraktionsvize Konstantin von Notz und Helge Limburg, Sprecher für Rechtspolitik, verlangten: „Die Vorratsdatenspeicherung gehört auf die Müllhalde der Geschichte". Sie stelle alle Bürger unter Generalverdacht – und habe die in sie gesetzten sicherheitspolitischen Erwartungen nie erfüllen können. Dass die einschlägigen Gesetzesklauseln trotz der seit Langem bekannten Linie der EuGH-Rechtsprechung bislang nur ausgesetzt seien, bezeichneten sie als „rechtspolitisch höchst fragwürdiges Vorgehen". Weiter: „Für eine – wie auch immer geartete – Neuauflage der Vorratsdatenspeicherung sehen wir weder rechtlichen noch politischen Spielraum." Sie begrüßten, dass der Bundesjustizminister im Einklang mit dem Koalitionsvertrag und den „zwischen den Häusern intensiv abgestimmten Vorhabensplanungen" bereits gemeinsam mit dem Innenministerium an einem Gesetzentwurf

für eine Quick-Freeze-Regelung arbeite. Es sei überfällig die ebenfalls vereinbarte Überwachungsgesamtrechnung auf den Weg zu bringen und „insgesamt eine zielgerichtete Sicherheitspolitik" zu verfolgen.

Das Ampel-Bündnis hat vereinbart: „Angesichts der gegenwärtigen rechtlichen Unsicherheit, des bevorstehenden Urteils des Europäischen Gerichtshofs und der daraus resultierenden sicherheitspolitischen Herausforderungen werden wir die Regelungen zur Vorratsdatenspeicherung so ausgestalten, dass Daten rechtssicher anlassbezogen und durch richterlichen Beschluss gespeichert werden können" (vgl. DANA 1/2022, 22 f.).

• Reaktionen aus der Wirtschaft

Eco-Geschäftsführer Alexander Rabe erklärte: „Wir haben als eco-Verband der Internetwirtschaft sechs Jahre für dieses Urteil mit unserem Mitgliedsunternehmen SpaceNet AG gekämpft." Jetzt sei es an der Zeit für die Bundesregierung „konsequent ihren eigenen Koalitionsvertrag umzusetzen und Abstand von diesem Instrument zu nehmen." Für die SpaceNet AG, die die Klage angestrengt hatte, begrüßte der Vorstand Sebastian von Bomhard das Urteil: „Nach sechs Jahren Verfahren sind wir froh, dass das Thema Vorratsdatenspeicherung endlich geklärt ist. Jetzt herrscht wieder Rechtssicherheit für die Internetbranche, unsere Kunden und alle Bürger." Es gebe geeignetere Mittel wie Quick Freeze, „um gegen schwere Kriminalität vorzugehen".

Auch Bernhard Rohleder, Geschäftsführer des IT-Verbands Bitkom, hofft, mit dem Urteil „beerdigt der EuGH faktisch die Vorratsdatenspeicherung". Es ergebe keinen Sinn sich weiter an diesem Instrument abzuarbeiten. Die Politik müsse „andere und zwar gesetzeskonforme Möglichkeiten der digitalen Forensik" nutzen.

• Bürgerrechtler und Datenschützer

Der Bundesdatenschutzbeauftragte Ulrich Kelber reagierte wie folgt: „Mein großer Wunsch: Ab heute endgültig Schluss mit Debatten über anlasslose Vorratsdatenspeicherungen." Stattdessen sollten Instrumente gestärkt werden, „die helfen, ob präventiv oder bei der Strafverfolgung", ohne dabei Grundrechte infrage zu stellen. Henning Tillmann vom der SPD nahestehenden digitalpolitischen Verein D64 empfahl der Innenministerin Faeser, sie müsse nun überlegen, ob sie den „gescheiterten Kult" und die „verfehlte Ideologie ihrer Vorgänger" im Innenministerium fortsetzen oder etwas für Opfer tun wolle. Sie solle neu denken und „rechtssichere Instrumente" wie die Login-Falle umsetzen.

Über 20 zivilgesellschaftliche Organisationen warnten am Tag vor dem Urteil unter der Ägide des Arbeitskreises gegen Vorratsdatenspeicherung in einem offenen Brief an die Ampel-Koalition, auch ein anlassloses Protokollieren von IP-Adressen wäre „zum Schutz von Kindern ungeeignet und ein schwerer Eingriff in Grundrechte" (in diesem Heft S. 254).

Sebastian Marg vom Verein Digitale Gesellschaft, der den Brief mit unterzeichnet hat, erklärte: „Es wird Zeit, dass die politisch Verantwortlichen die Vorratsdatenspeicherung ein für alle Mal begraben und statt dessen grundrechtskonforme Alternativen entwickeln". Die langjährigen Auseinandersetzungen hätten nicht nur zu einer massiven Verunsicherung über die geltende Rechtslage geführt, sondern auch gezeigt, dass eine anlasslose Massenüberwachung das Gegenteil einer den Grundrechten der Bevölkerung verpflichteten Politik sei.

Padeluun vom Verein Digitalcourage, der eine noch laufende Verfassungsbeschwerde mit ins Rollen gebracht hat, meinte, das anlasslose Protokollieren von Verbindungs- und Standortdaten „ist keine rechtsstaatliche Ermittlungsmaßnahme, sondern – egal, wie man es dreht oder wendet – eine grundrechtswidrige Massenüberwachung der gesamten Bevölkerung". Die Politik müsse sich von „jeglicher Vorratsdatenspeicherung verabschieden" statt sie ständig in neuem Gewand wiederzubeleben.

Und Christine Regitz, Präsidentin der Gesellschaft für Informatik (GI), hob hervor, dass das verdachtsunabhängige Sammeln von Verkehrsdaten gravierend in die Privatsphäre eingreift und Bürger sowie IT-Wirtschaft gleichermaßen verunsichert: „Sie untergräbt das Vertrauen in sichere Internetkommunikation und gefährdet dadurch die dringend notwendige Digitalisierung von Wirtschaft und Verwaltung." Anstatt dieses tote Pferd weiterzureiten, sollte die Bundesregierung dringend datensparsamere Alternativen entwickeln (Weiß, EuGH bestätigt: keine anlasslose Vorratsdatenspeicherung – mit Ausnahmen, www.heise.de 21.09.2022; Kurzlink: https://heise.de/-7269443; Krempl, Nach EuGH-Urteil: Bayern drängt auf Vorratsspeicherung von IP-Adressen, www.heise.de 21.09.2022, Kurzlink: https://heise.de/-7269995; Deutsche Vorratsdatenspeicherung verstößt gegen EU-Recht, www.sueddeutsche.de 20.09.2022; Janisch, Ein bisschen geht schon, SZ 21.09.2022, 2).

EuGH

Einwilligungen und Betroffenenansprüche wirken für viele Verantwortliche

Gemäß einem Urteil des Europäischen Gerichtshofes (EuGH) vom 27.10.2022 muss ein für die Verarbeitung personenbezogener Daten Verantwortlicher auch nach deren Weitergabe dafür Sorge tragen, dass sie auf Antrag auch bei den Empfängern gelöscht werden (Az. C-129/21). Das umfangreiche Löschen persönlicher Daten aus Verzeichnissen wie Telefonbüchern könnte nach diesem Urteil künftig wesentlich einfacher werden. Haben Telefonanbieter die Kundendaten an andere Anbieter oder an Suchmaschinen weitergegeben, müssen sie auch dafür sorgen, dass dort die Einträge gelöscht werden, wenn die Kunden sie darum bitten. Die Verantwortlichen müssen – als technisch-organisatorische Maßnahme – die Daten vorhalten, die nötig sind, um diesen Wünschen zu entsprechen. Die Betroffenen müssen die Löschung nicht bei jedem Unternehmen einzeln beantragen.

Hintergrund des Urteils ist ein Verfahren gegen den belgischen Telefonanbieter Proximus, der unter anderem Telefonauskunftsdienste und Verzeichnisse mit Namen, Adressen und Telefonnummern anbietet. Diese werden von anderen Anbietern an Proximus übermittelt und Proximus leitet sie auch an andere Anbieter und Suchmaschinen wie Google weiter. Dafür wurde nur eine einzige

Einwilligung der Kunden eingeholt, was auch genügt.

Ein Kunde wehrte sich dagegen, dass seine neue Telefonnummer in einem solchen Verzeichnis stand, ohne dass er eingewilligt hatte. Proximus argumentierte, dass die Einwilligung des Kunden für die Veröffentlichung seiner Daten in Telefonverzeichnissen nicht erforderlich sei. Vielmehr müssten sie nach einem sogenannten Opt-out-Verfahren ausdrücklich beantragen nicht aufgeführt zu werden. Solange das nicht geschehe, müssten Daten nicht gelöscht werden. Dem folgte der EuGH nicht. Bevor die Daten veröffentlicht werden, müssen die Kunden einwilligen. Durch diese Einwilligung könnten dann zwar auch andere Unternehmen die Daten verarbeiten, sofern damit der gleiche Zweck verfolgt wird. Genauso reicht es dann aber aus nur ein einziges Mal seine Einwilligung zu widerrufen – egal ob gegenüber dem eigenen Anbieter oder einem der anderen Unternehmen, die die Daten verwenden. Die Telefonanbieter sind dann verpflichtet den Widerruf weiterzuleiten und dafür zu sorgen, dass die Daten gelöscht werden.

OLG Karlsruhe

US-Töchter sind von Vergabeverfahren nicht ausgeschlossen

Deutsche Behörden dürfen gemäß einem rechtskräftigen Beschluss des Oberlandesgerichts Karlsruhe (OLG) vom 07.09.2022 im sofortigen Beschwerdeverfahren bei öffentlichen Aufträgen weiterhin auf Tochtergesellschaften von US-amerikanischen Cloud-Dienste-Anbietern zurückgreifen, wenn diese zusichern die Daten in Deutschland zu verarbeiten (Az. 15 Verg 8/22): Die Anbieterin eines digitalen Entlassmanagements für Patienten ist nicht allein deswegen aus einem Vergabeverfahren zweier kommunaler Krankenhausgesellschaften auszuschließen, weil sie die luxemburgische Tochtergesellschaft eines US-amerikanischen Unternehmens als Hosting-Dienstleisterin einbindet. Das OLG hob damit eine Entscheidung der Vergabekammer Baden-Württemberg vom 13.07.2022 auf (s.u.). Amazon, Microsoft oder Google dürfen danach weiter auf Aufträge deutscher Behörden hoffen. Die Vorinstanz hatte einen solchen Anbieter wegen datenschutzrechtlicher Bedenken aus dem Rennen geworfen und sich dabei auf das „latente Risiko" eines Zugriffs durch US-Behörden gestützt. Die Umsetzung dieser Entscheidung hätte große Cloud-Anbieter wie Amazon Web Services (AWS), Microsoft oder Google von der Zusammenarbeit mit deutschen Behörden kategorisch ausgeschlossen.

Gemäß dem OLG dürfen sich öffentlichen Auftraggeber auf die bindenden Zusagen der Anbieterin verlassen, dass die Daten ausschließlich in Deutschland verarbeitet und in kein Drittland übermittelt werden. Grundsätzlich sei davon auszugehen, dass ein Bieter seine vertraglichen Zusagen erfüllen werde. Erst wenn sich aufgrund konkreter Anhaltspunkte Zweifel daran ergäben, müsse der öffentliche Auftraggeber ergänzende Informationen einholen und die Erfüllbarkeit des Leistungsversprechens prüfen.

Christian Schröder, Anwalt der Kanzlei Orrick, Herrington & Sutcliffe, der nicht an dem Verfahren beteiligt war, meinte: „Das ist ein Schritt zurück in die Normalität". Alles andere hätte zu großer Unsicherheit geführt. Cloud-Diensteanbieter aus den USA wie AWS und Microsoft stellten wegen der Entscheidung des Europäischen Gerichtshofs zu Schrems II (DANA 3/2020, 199 ff.) ihre Geschäftsmodelle um und bieten nunmehr über europäische Tochtergesellschaften Serverfarmen mit Standorten in Deutschland oder dem europäischen Ausland an. Ziel ist es den strengen Anforderungen des europäischen Datenschutzes gerecht zu werden. Die Vergabekammer hatte sich jedoch zuvor auf den Standpunkt gestellt, dass dies nicht ausreicht. Sie fürchtete auch in diesen Konstellationen, dass amerikanische Behörden auf die personenbezogenen Daten europäischer Bürger zugreifen könnten. Nach Einschätzung der Vergabekammer könne sich dieses latente Risiko „jederzeit realisieren" (Budras, Oberlandesgericht Karlsruhe hegt den Datenschutz ein, www.faz.net 07.09.2022; OLG Karlsruhe: Auftraggeber dürfen sich auf bindende Zusagen verlassen – auch zum Datenschutz, www.vergabeblog.de 08.09.2022).

VK Baden-Württemberg

US-Cloud-Tochter von der Vergabe ausgeschlossen

Die Vergabekammer Baden-Württemberg (VK) – eine gerichtsähnliche, beim Regierungspräsidium Karlsruhe angesiedelte Instanz im Vergaberecht – hat mit ihrem nicht rechtskräftigen Beschluss vom 13.07.2022 entschieden, dass die EU-Tochter einer US-Firma nicht an einem Vergabeverfahren teilnehmen darf, weil sie Daten in die USA übermitteln könnte; ob sie es tut, sei unerheblich (Az. 1 Vk 23/22). Das in der EU ansässige Tochterunternehmen eines US-Anbieters für Server- und Cloud-Dienstleistungen hatte sich an einem Vergabeverfahren beteiligt. Obwohl sich die zur Leistungserbringung eingesetzten Server innerhalb der EU befanden, stellte die Vergabekammer einen Verstoß gegen die Datenschutz-Grundverordnung fest. Durch diesen Verstoß sei ein entsprechendes Angebot aus dem Vergabeverfahren auszuschließen, da es nicht den Vergabeunterlagen entspricht. Dies ist der Fall, da die Anbieterin „keine mit dem anwendbaren Datenschutzrecht zu vereinbarende Leistungserbringung anbietet".

Nach der Entscheidung genügt die bloße Möglichkeit des Zugriffs auf personenbezogene Daten durch das US-Mutterunternehmen, um eine Übermittlung in die USA zu unterstellen. Die bloße Möglichkeit genüge: „Eine in diesem Zusammenhang berücksichtigungsfähige Offenlegung ist auch dann anzunehmen, wenn eine Einstellung personenbezogener Daten auf eine Plattform erfolgt, auf die von einem Drittland aus zugegriffen werden kann, und zwar unabhängig davon, ob der Zugriff tatsächlich erfolgt." Auf den physischen Standort des Servers komme es nicht an.

Die VK kommt in ihrem Beschluss auch zu dem Ergebnis, dass die Verwendung der so genannten EU-Standarddatenschutzklauseln im konkreten Fall nicht ausreicht, um einen Verstoß gegen die DSGVO auszuschließen. Selbst die Verpflichtung gegen etwaige staatliche Anordnungen auf Zugriff auf personenbezogene Daten durch Anfechtung vorzugehen, „beseitigt das latente Risiko eines Zugriffs durch ebendiese Stellen nicht".

Hätte der Beschluss der VK Bestand gehabt (dazu s.o. das OLG Karlsruhe), so

wären US-Konzerne selbst dann von Vergabeverfahren auszuschließen gewesen, wenn sie Server zur Verarbeitung personenbezogener Daten innerhalb der EU durch Tochterunternehmen bereitstellen. Letztlich hat diese Frage auch Auswirkungen auf die Zusammenarbeit privater Unternehmen mit solchen Diensteanbietern, denn die datenschutzrechtliche Beurteilung hängt nicht davon ab, ob staatliche Stellen oder private Unternehmen derlei Dienste in Anspruch nehmen.

Hintergrund des Verfahrens ist die Entscheidung des Europäischen Gerichtshofs vom 16.07.2020. Darin hatte dieser Übermittlungen personenbezogener Daten auf Basis des EU-US Privacy Shield untersagt (Schrems-II, DANA 3/2020, 199 ff.). Die EU-Kommission und zuständige Stellen in den USA arbeiten an einem Nachfolgeabkommen (siehe hierzu den Artikel von Weichert auf S. 246). Mit einem Abschluss und einer anschließenden sogenannten Angemessenheitsentscheidung der EU-Kommission ist nicht vor Ende 2022 zu rechnen.

Die Entscheidung der Vergabekammer wurde erfolgreich vor dem Oberlandesgericht Karlsruhe angegriffen (s.o.). Hätte sie Bestand gehabt, so wären die größten Cloud-Anbieter wie Amazon Web Services (AWS), Microsoft und Google trotz neuer Modelle mit Rechenzentren in der EU von der künftigen Kooperation mit deutschen Behörden weitgehend ausgeschlossen gewesen. Der baden-württembergische Datenschutzbeauftragte Stefan Brink bezeichnet den VK-Beschluss zwar als „sachlich qualifiziert“. Dieser habe eine über ein behördliches Vergabeverfahren hinausweisende Bedeutung. Doch wendete er ein, dass das Verfahren Vereinbarungen zum Gegenstand hatte, die aus Sicht der Vergabekammer noch hinter den Anforderungen der aktuell einsetzbaren Standarddatenschutzklauseln zurückbleiben. Hier scheine „nicht durchgängig der Zugriff auf die jeweils einschlägige Vertragsklausel gelungen zu sein“. Das sei angesichts der Komplexität der einzubeziehenden Regularien auch nicht verwunderlich.

Brink hält es für „rechtlich zweifelhaft“, dass die Kammer das Zugriffsrisiko und eine Datenweitergabe an US-Behörden gleichsetzte. Dass die DSGVO einen „risikobasierten Ansatz“ zugunsten Verantwortlicher eingeführt habe, werde von interessierten Kreisen zwar immer wieder pauschal vorgebracht. Es überzeuge aber nicht, dass ein solcher auch noch zulasten von Daten verarbeitenden Stellen „umgedreht werden dürfte“. Die Kammer habe übersehen, dass gegen die erwähnten Zugriffsrisiken wirksame Gegenmittel in Gestalt „technisch-organisatorischer Maßnahmen“ existierten, die letztlich jede einschlägige Gefahr ausschließen könnten. Dazu gibt es eine Orientierungshilfe der Aufsichtsbehörde.

Der Rechtsanwalt Stephan Schmidt von der Mainzer Kanzlei TCI hielt die Entscheidung ebenfalls für „überzogen und schlecht begründet“: Die Juristen der Kammer hätten nicht berücksichtigt, dass US-Firmen und deren Mitarbeiter gegen die DSGVO verstießen und so selbst mindestens eine Ordnungswidrigkeit begingen, sollten sie personenbezogene Informationen einfach herausgeben. Der österreichische Aktivist Max Schrems, der das EuGH-Grundsatzurteil auslöste, beklagt derweil, dass bislang getroffene Vorkehrungen zum Ergänzen von Standardvertragsklauseln meist nicht ausreichten (https://rewis.io/urteile/urteil/ocw-13-07-2022-1-vk-2322/; Haar, Cloud-Dienste: Vergabekammer verbietet Angebot von US-Tochterunternehmen, www.heise.de 05.08.2022, Kurzlink: https://heise.de/-7204620; Krempl, Cloud: Datenschützer hält Ausschluss von US-Firmentöchtern für zweifelhaft, www.heise.de 15.08.2022, Kurzlink: https://heise.de/-7220725).

VG Berlin

1. Mai-Demonstrations-Videoüberwachung aus Schutzgründen zulässig

Das Verwaltungsgericht Berlin (VG) entschied mit Urteil vom 22.08.2022, dass die Videoüberwachung von ca. 7.500 Demonstrationsteilnehmenden durch die Bundespolizei mit schwenkbaren Zoomkameras am S-Bahnhof Grunewald im Zusammenhang mit den Demonstrationen anlässlich des 1. Mai im Jahr 2019 rechtmäßig gewesen sei (Az. 1 K 405/20). Es habe ein ähnliches Gefahrenpotenzial wie beim Loveparade-Unglück in Duisburg bestanden. Damit blieb die Klage von Veranstaltern einer Versammlung erfolglos, die am S-Bahnhof im Berliner Villenviertel Grunewald startete und endete.

Ziel der Videoaufzeichnung sei die Sicherheit am beengten Bahnhof gewesen. Die Bundespolizei habe – auch mit Blick auf Erfahrungen aus dem Vorjahr – rechtzeitig erkennen wollen, ob eine Überfüllung des Bahnsteigs und des Personentunnels drohe.

Eine dem § 27 Bundespolizeigesetz entsprechende Gefahr, die den Kameraeinsatz erlaubt, bestand aus Sicht des Gerichts angesichts der engen räumlichen Situation am S-Bahnhof und der Vielzahl von Menschen, die zu erwarten gewesen seien. Das Gericht bezog sich, der Argumentation der Polizei folgend, auf die Erfahrungen bei der Loveparade in Duisburg im Jahr 2010, wo es zu einer Katastrophe mit 21 Toten und Hunderten Verletzten gekommen war, weshalb der Eingriff in die Versammlungsfreiheit und das Recht auf informationelle Selbstbestimmung gerechtfertigt sei. Die Videoüberwachung sei auf Bahnsteigen, Treppenabgängen und im Empfangsbereich – nicht aber auf dem Bahnhofsvorplatz – erfolgt. Es sei mit mehreren Schildern auf die Kameras hingewiesen worden. Am 15.05.2019 seien die Aufzeichnungen schließlich von der Polizei gelöscht worden.

Frauke Geldher, Sprecherin des Quartiersmanagement Grunewald kündigte an: „Das Urteil des VG Berlin bedeutet eine Schwächung des Versammlungsrechts gegen staatliche Eingriffe. Dies ist nicht hinnehmbar. Wir beantragen deswegen die Zulassung der Berufung zum Oberverwaltungsgericht Berlin-Brandenburg. Aus dem Verwaltungsvorgang ergibt sich eindeutig, dass die Sorge um einen zu vollen Bahnhof nicht der Grund für die Videoüberwachung war.“ So sei zum Ziel der Videoüberwachung von „Beweissicherung“ die Rede gewesen; ferner habe die Bundespolizei u.a. bei der Berliner Landespolizei angefragt, ob Bedarf an den Aufzeichnungen bestünde – offensichtlich zur weiteren Speicherung und Auswertung. „Mit der akuten Abwehr von Gefahren durch einen überfüllten Bahnhof hat all dies nichts zu tun. Dass das Gericht dies nicht erkennen will, ist nicht nachvollziehbar“ (Videoüberwachung am Bahnhof aus Sicherheitsgründen zulässig, www.lto.de 19.09.2022; QM-Grunewald und FIfF, Videoüberwachung am 1. Mai 2019 in Berlin-Grunewald: Berufung gegen Urteil des VG Berlin, PE v. 20.09.2022).

Buchbesprechungen

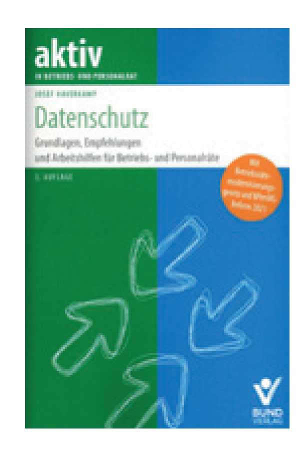


Assion, Simon (Hrsg.)
TTDSG Telekommunikations-Telemedien-Datenschutz-Gesetz
Handkommentar
Nomos Verlag, Baden-Baden, 1. Aufl. 2022, ISBN 978-3-8487-7054-0, 554 S, 109,00 €

(tw) Das TTDSG ist seit dem 01.12.2021 in Kraft. Gemäß der Tradition im allgemeinen Datenschutzrecht ist dazu zeitnah schon viel Literatur erschienen, die das neue Gesetz kommentiert. Inzwischen gibt es drei selbstständige Kommentare dazu – der von Assion herausgegebene ist einer – sowie weitere, die das TTDSG in Kombination mit der DSGVO und dem BDSG kommentieren. Auch Aufsätze gibt es schon eine ansehnliche Menge. Und dies ist gut so, da die behandelte Materie nicht gerade anwendungsfreundlich ist: „Das TTDSG war trotz langer Vorbereitungszeit nur wenig ausgereift, als es vom Bundestag verabschiedet wurde, und manche Vorschriften ... müssen in der Praxis erst noch ankommen. Andere ... sind im Wortlaut veraltet und auf moderne Telekommunikationstechnologien kaum noch praktikabel anwendbar. Eine große Herausforderung für unsere Autorinnen und Autoren!“ Die Feststellung der Herausforderung durch den Herausgeber, der sich der Rezensent anschließt, wurde von den 14 Autorinnen und Autoren – weitestgehend aus der Anwaltschaft – beherzigt. Sie schaffen es, die sperrige Materie soweit zu entsperren, dass das Gesetz anwendbar wird. Das Werk geht offenen Fragen nicht aus dem Weg und gibt eigene Antworten – unter Darstellung möglicher Gegenpositionen. Es geht zumindest dogmatisch in die verfassungsrechtliche Tiefe und beschreibt die vielen Querbezüge zu anderen Gesetzen, allen voran die ePrivacy-Richtlinie und die DSGVO sowie viele weitere europäische und nationale sowie auch bundeslandspezifische Normen. Es zeigt die wechselvolle Geschichte der einzelnen Regelungen auf – vom Telegraphengeheimnis von 1892, vor allem seit den 1990er Jahren mit Telekommunikationsdienstunternehmen-Datenschutzverordnung, Telekommunikations-Datenschutzverordnung, Telekommunikationsgesetz (TKG), Teledienstedatenschutzgesetz und Telemediengesetz (TMG) bis nun zum TTDSG, das zu einem noch nicht absehbaren Zeitpunkt zumindest teilweise von der seit Jahren angekündigten und politisch streitigen europäischen ePrivacy-Verordnung abgelöst werden wird. Eine Stärke der Kommentierungen besteht darin, dass auf die Erfahrungen mit den Vorgängergesetzen zurückgegriffen wird, was sich anbietet, zumal die Hauptregelungen des TTDSG die Datenschutznormen des früheren TKG und TMG sind, die für Netzanbieter und Telemedienanbieter galten und auch weiterhin – bei allen Überschneidungen – in getrennten Abschnitten des TTDSG zu betrachten sind.

Die vielen Verweise auf – auch die aktuelle – Literatur geben denjenigen, die es noch genauer wissen wollen, Ansatzpunkte für Vertiefungen, wobei diese dank der Darstellung auch fremder Positionen oft gar nicht nötig ist. Die vertretenen Standpunkte sind durchgängig vertretbar, auch wenn man sich nicht immer diesen anschließen mag, etwa wenn die Anwendbarkeit des Fernmeldegeheimnisses durch Arbeitgeber bei erlaubter Privatnutzung am Arbeitsplatz behauptet wird. Der Kommentar ist durchgängig der juristischen Dogmatik verhaftet; die technischen oft sehr komplexen Hintergründe werden allenfalls angerissen. Angesichts der technischen Vielfalt im Bereich der digitalen Kommunikation bleiben so praktische Fragen manchmal offen, so dass weitere Quellen herangezogen werden müssen. Technische Vorkenntnisse sind bei der Kommentarnutzung oft nötig.

Wer also mit dem TTDSG viel zu tun hat, dem sei dieser Kommentar empfohlen. Er schafft etwas Ordnung in die bestehende regulative Unordnung. Es bleibt aber weiterhin zu hoffen, dass das TTDSG bald durch eine einheitliche europäische Regelung, die ePrivacy-Verordnung, ersetzt wird, die dann auf die DSGVO abgestimmt ist. Es werden aber auch dann Restbestände des aktuellen TTDSG übrigbleiben, die möglicherweise überleben – etwa die zu den Rechten der Erben (§ 4) oder zu den Personal Informations Managements Systems (PIMS, § 26) oder die behördlichen Zugriffsnormen auf Verkehrs- und Bestandsdaten (§§ 21 ff.).



Haverkamp, Josef
Datenschutz – Grundlagen, Empfehlungen und Arbeitshilfen für Betriebs- und Personalräte
Bund Verlag, 3. umfassend überarbeitete und aktualisierte Aufl. 2022, Frankfurt am Main; 420 S., 32,00 €. ISBN 978-3-7663-7072-3.

(hdn) Autor Josef Haverkamp wird in diesem Buch als Fachjournalist für IT-Fragen mit den Schwerpunkten Da-

tenschutz und Digitalisierung, Zertifizierter Datenschutzbeauftragter und Referent bei Datenschutz- und IT-Seminaren vorgestellt.

Schon das erste Durchblättern macht deutlich, dass die Versprechen, die der Titel liefert, in dem kompakten Buch aus dem für diese Belange spezialisierten Bund-Verlag stringent eingehalten werden. Der Inhalt wendet sich an die Menschen, die in verschiedenen Mitarbeitervertretungen ihrer Betriebsrat- und Personalratstätigkeit nachgehen und die die bislang eher ungeklärten datenschutzrechtlichen Verpflichtungen berücksichtigen müssen.

Dabei hat Haverkamp nicht nur die aktuelle Gesetzeslage (Novellierung des Betriebsverfassungsgesetzes und des Bundespersonalvertretungsgesetzes von 2021) eingepflegt, sondern geht auch umfassend und intensiv auf die Anforderungen von DSGVO und BDSG, BetrVG und BPerVG (einschl. Ländergesetze) ein. Die angewandte Semantik und grafische Ausgestaltung helfen Leserin und Leser bei der Erfassung der nicht immer einfachen datenschutzrechtlichen Inhalte. Der Text ist in der Tat sehr verständlich verfasst, eindeutige Icons helfen beim Auffinden von Checklisten und gute Tabellen stellen verschiedene Anforderungen zum Beispiel bei den PVerVG der Länder gegenüber.

Die Textpassagen in den Kapiteln beschreiben die Gesetzeslage zum Teil sehr umfassend und schließen mit Hinweisen auf Rechtsgrundlagen und Literatur ab. Die überaus sparsame Verwendung juristischer Fachtermini dürfte bei der Zielgruppe zudem hohen Anklang finden. Hervorhebungen machen auf wichtige Aspekte und Besonderheiten aufmerksam. Zur praktischen Anwendung werden Muster zum Beispiel für Einwilligungen oder zum Widerruf einer Einwilligung angeboten.

Der Bleistift am Rand der Texte führt zu Checklisten, die teilweise sehr umfassend ausfallen. Die Bestandsaufnahme zum Datenschutz im Büro der Interessenvertretung beispielsweise umfasst mehr als sechs Buchseiten. Insgesamt gibt es 23 dieser Checklisten, die meisten wurden für die Einhaltung technischer Schutzmaßnahmen erstellt. Gleich ein ganzes Kapitel beschreibt den „Weg zum Datenschutz der Interessenvertretung in fünf Schritten“. Eine besondere Rolle kommt dabei dem Sonderbeauftragten für den Datenschutz zu, der in der Interessenvertretung tätig werden muss.

Eine weitere Besonderheit in diesem Buch stellt die Beschreibung der Arbeit von BeDaX dar, einem wissenschaftlich fundierten Instrument zur Bewertung des Beschäftigtendatenschutzes in Betrieb, Unternehmen oder Verwaltung.

Das Buch von Josef Haverkamp sollte in jedem Büro einer Interessenvertretung verfügbar sein.



Sydow, Gernot/Marsch, Nikolaus (Hrsg.)
DS-GVO | BDSG
Nomos Verlag Baden-Baden,
3. Auflage 2022, 2559 S.,
ISBN 978-3-8487-7290-2, 189,00 €

(me) Der Handkommentar erscheint – verdientermaßen – in nunmehr 3. Auflage und wird in Deutschland (Nomos Verlagsgesellschaft), der Schweiz (Dike Verlag) und Österreich (Manz'sche Verlags- und Universitätsbuchhandlung) verlegt.

Die Veröffentlichung der Kommentierung von DSGVO und BDSG in einem Band ist nicht neu. Es gibt andere Kommentare, die dieses Konzept ebenfalls verwenden. In diesem Fall ist es besonders gut gelungen: Lobend zu erwähnen ist insbesondere die Einleitung von Gernot Sydow, in der sehr schön dargestellt wird, wie sich das Datenschutzrecht in einem Mehrebenensystem entfaltet und wie der jeweilige Regelungsgehalt von DSGVO, TTDSG und BDSG vor dem Hintergrund der datenschutzgrundrechtlichen Gewährleistung durch Art. 8 EU-Grundrechte-Charta und Art. 16 AEUV zu verstehen ist. Die Ausführungen gehen über das üblicherweise von einer Einführung zu Erwartende hinaus. Auf verständliche und dogmatisch überzeugende Weise werden die Regelungsspielräume der Mitgliedsstaaten dargestellt und erläutert. Im Weiteren von hohem Interesse sind die Bewertungen neuer Herausforderungen wie beispielsweise der sog. Künstlichen Intelligenz (KI), der Blockchain-Technik sowie der Ausblick auf ausländische (=außereuropäische) Rechtsordnungen wie den kalifornischen Consumer Privacy Act, das brasilianische Datenschutzgesetz und das japanische Regularium. Auch einem Lehrbuch zum Datenschutzrecht würde es gut zu Gesicht stehen eine Einleitung dieser Qualität zu enthalten.

Besonders gut sind die Kommentierungen von Ingold zu Art. 28 DSGVO (Auftragsverarbeitung) und von Towfigh und Ulrich zu Art. 46 ff. DSGVO (Datenübermittlung an Drittländer) gelungen, die dem praktischen Anwender das nötige Rüstzeug liefern. In diesem Zusammenhang wird das EuGH-Urteil „Schrems-II“ dargestellt.

Mit Beifall zu bedenken sind die Darstellungen der insgesamt 30 Autoren des Handkommentars zu aktuellen datenschutzrechtlichen Themen wie beispielsweise dem Beschäftigtendatenschutz in Art. 26 BDSG (kommentiert von Tiedemann), dem Auskunftsrecht gem. §§ 57, 34 BDSG (kommentiert von Bienemann) und zur Videoüberwachung öffentlicher Räume gem. § 4 BDSG (kommentiert von Marsch). Das im Vorwort gesetzte Ziel der Erarbeitung von Lösungen zu Anwendungsfragen des materiellen Datenschutzrechts wird erreicht: Im Bücherregal des in der Praxis mit Datenschutzfragen Beschäftigten sollte dieser Handkommentar nicht fehlen. Zu bemängeln wäre die Qualität des Papiers, die etwas zu dünn geraten scheint. Vielleicht ist bei dieser – nur das äußere Erscheinungsbild des Werkes betreffenden – Kritik Nachbesserung möglich.

Freiwillige Gegendarstellung

Im letzten Heft (DANA 3/2022) hielten wir folgenden Witz für angebracht:



Mit der Fußnote wollten wir klarstellen, dass die aktuelle Innenministerin Faeser in diesen Witz nicht mit einbezogen werden sollte, weil sie erst ein gutes halbes Jahr im Amt war und wir (auch vor dem Hintergrund des aktuellen Koalitionsvertrages) die Hoffnung hatten, dass sie sich in dem Punkt (Einsatz für Datenschutz und andere Grundrechte) von ihren Vorgängern unterscheiden würde.

Für diese Naivität unsererseits (die Redakteure der DANA 3/2022) wollen wir uns hiermit bei unseren Lesern aufrichtig entschuldigen.